CONWAY GROUPOIDS AND COMPLETELY TRANSITIVE CODES

NICK GILL, NEIL I. GILLESPIE, AND JASON SEMERARO

ABSTRACT. To each supersimple $2-(n,4,\lambda)$ design $\mathcal{D}$ one associates a 'Conway groupoid,' which may be thought of as a natural generalisation of Conway's Mathieu groupoid M_{13} which is constructed from $\mathbb{P}_3$.

We show that $\mathrm{Sp}_{2m}(2)$ and $2^{2m}.\mathrm{Sp}_{2m}(2)$ naturally occur as Conway groupoids associated to certain designs. It is shown that the incidence matrix associated to one of these designs generates a new family of completely transitive $\mathbb{F}_2$-linear codes with minimum distance 4 and covering radius 3, whereas the incidence matrix of the other design gives an alternative construction of a previously known family of completely transitive codes.

We also give a new characterization of M_{13} and prove that, for a fixed $\lambda > 0$, there are finitely many Conway groupoids for which the set of morphisms does not contain all elements of the full alternating group.

1. INTRODUCTION

In recent work with A. Nixon [12], we introduced the notions of a *puzzle set* and *hole stabiliser* associated to a supersimple $2-(n,4,\lambda)$ design $\mathcal{D}$, i.e. a $2-(n,4,\lambda)$ design for which any two lines intersect in at most two points. In this paper we introduce the concept of a *Conway groupoid* which is a direct generalization of the groupoid associated to Conway's famous construction of M_{13} using a 'game' played on $\mathbb{P}_3$, the finite projective plane of order 3 [7].

The Conway groupoid $\mathcal{C}(\mathcal{D})$ of $\mathcal{D}$ is a small category whose set of objects is the set of points in $\mathcal{D}$, and whose morphisms can be 'read off' from the lines in $\mathcal{D}$; in particular, this process associates an element of the group $\mathrm{Sym}(n)$ to each morphism in $\mathcal{C}(\mathcal{D})$ (see Section 2 for full details). For example, by viewing $\mathbb{P}_3$ as a supersimple $2-(13,4,1)$ design, the set M_{13} inside $\mathrm{Sym}(13)$ determines a Conway groupoid. A number of other examples were constructed in [12]. In this paper we are interested in constructing more examples of Conway groupoids and in working towards a full classification.

Constructing examples: We say that a Conway groupoid $\mathcal{C}$ associated to a supersimple $2-(n,4,\lambda)$ design is *full* if every element of $\mathrm{Alt}(n)$ occurs as a morphism. One of the main results in [12] suggests that those designs whose Conway groupoids are not full are rare [12, Theorem C]. In this paper, we demonstrate the

2010 *Mathematics Subject Classification.* 20B15, 20B25, 05B05.

Key words and phrases. primitive groups, symmetric generation, completely regular codes, completely transitive codes, symplectic groups, Conway groupoids, Mathieu groupoid.

Part of the work for this paper was completed while Nick Gill was a visiting professor at the Universidad de Costa Rica. He would like to thank the mathematics department there for their warm hospitality. In addition, all three authors would like to thank Professor Noam Elkies for answering our questions about M_{13}, and an anonymous referee for pointing out several inaccuracies in an earlier version of the paper.

existence of two infinite families of designs with this property. These families arise from:

(a) the two 2-transitive actions of $\mathrm{Sp}_{2m}(2)$ on sets of quadratic forms over a $2m$-dimensional $\mathbb{F}_2$-vector space, for $m \geqslant 3$;
(b) the natural action of the affine group $2^{2m}.\mathrm{Sp}_{2m}(2)$ on $(\mathbb{F}_2)^{2m}$.

Both actions give rise to codes associated to the incidence matrices of the corresponding designs. In case (b), these codes were already known (see [3]). However, in case (a) the codes which arise are new; they are completely transitive and have covering radius 3.

Classifying Conway groupoids: We prove two main results - Theorems D and E below - that give classifications of Conway groupoids subject to certain extra suppositions. Both results have interesting implications: Theorem D gives a new characterization of the Conway groupoid determined by M_{13}; Theorem E yields a proof of [12, Conjecture 8.1], which asserts that for each $\lambda > 0$ there exist only finitely many supersimple $2-(n, 4, \lambda)$ designs whose Conway groupoids are not full.

1.1. **The main theorems.** In this section we briefly outline the main results of the paper. The definitions of all terms used in the statement of these results can be found in Sections 2 and 3.

In order to construct new infinite families of Conway groupoids we study the action of the group $\mathrm{Sp}_{2m}(2)$ on the set Ω of quadratic forms $(\mathbb{F}_2)^{2m} \to \mathbb{F}_2$ polarising to the alternating form associated to $\mathrm{Sp}_{2m}(2)$. We make use of a bijection between Ω and the vector space $V \cong \mathbb{F}_2^{2m}$ on which $\mathrm{Sp}_{2m}(2)$ naturally acts, allowing us to denote quadratic forms by θ_a for some $a \in V$. (This bijection is fully explained in Section 3.)

For $\varepsilon \in \{0, 1\}$ write $V^\varepsilon := \{v \in V \mid \theta_0(v) = \varepsilon\}$ (here θ_0 is the quadratic form associated with the zero vector). Then the induced action of $\mathrm{Sp}_{2m}(2)$ on Ω splits into two orbits Ω^0 and Ω^1 where $\Omega^\varepsilon := \{\theta_a \mid a \in V^\varepsilon\}$. Our first result asserts the existence of some supersimple designs with these orbits.

Theorem A. *Let $m \geqslant 3$ and $\varepsilon \in \mathbb{F}_2$. Then*

$$\mathcal{B}^\varepsilon := \{\{\theta_{v_1}, \theta_{v_2}, \theta_{v_3}, \theta_{v_1+v_2+v_3}\} \mid v_i \in V^\varepsilon, \sum_{i=1}^{3} v_i \in V^\varepsilon\}$$

forms the line set for a supersimple $2-(f_\varepsilon(m), 4, f_\varepsilon(m-1)-1)$ design $(\Omega^\varepsilon, \mathcal{B}^\varepsilon)$ where

$$f_\varepsilon(m) := |\Omega^\varepsilon| = 2^{m-1} \cdot (2^m + (-1)^\varepsilon). \tag{1.1}$$

Furthermore, letting θ_0 be the quadratic form associated to the zero vector,

$$\mathcal{B}^a := \{\{v_1, v_2, v_3, v_1+v_2+v_3\} \mid v_i \in V, \sum_{i=1}^{3} \theta_0(v_i) = \theta_0\left(\sum_{i=1}^{3} v_i\right)\}$$

forms the line set for a supersimple $2-(2^{2m}, 4, 2^{2(m-1)}-1)$ design $(V, \mathcal{B}^a)$.

Let us write 2^{2m} for an elementary abelian group of order 2^{2m}. Then, as we shall see (Lemmas 3.8 and 3.11), the sets $\mathcal{B}^\varepsilon$ (resp. $\mathcal{B}^a$) are, in fact, orbits of the group $\mathrm{Sp}_{2m}(2)$ (resp. $2^{2m}.\mathrm{Sp}_{2m}(2)$) acting on the set of 4-subsets of Ω (resp. V). It turns out that this is not the first time that the action of $\mathrm{Sp}_{2m}(2)$ on the set of associated quadratic forms has been used to construct designs with special properties [25].

Write $\mathcal{D}^\varepsilon := (\Omega^\varepsilon, \mathcal{B}^\varepsilon)$ and $\mathcal{D}^a := (V, \mathcal{B}^a)$ for the designs constructed in Theorem A. Our next result, Theorem B, proves the existence of an infinite class of Conway groupoids; these are the Conway groupoids associated to $\mathcal{D}^a$ and $\mathcal{D}^\varepsilon$.

To understand the statement of the theorem we introduce some notation. Given a point ∞ in a design $\mathcal{D}$, we write $\mathcal{L}_\infty(\mathcal{D})$ for the set of all move sequences in $\mathcal{D}$ which start at ∞, while we write $\pi_\infty(\mathcal{D})$ for the set of all move sequences which start and end at ∞. Writing n for the number of points in $\mathcal{D}$, we observe that $\mathcal{L}_\infty(\mathcal{D})$ is a subset of $\mathrm{Sym}(n)$, while $\pi_\infty(\mathcal{D})$ is a subgroup of $\mathrm{Sym}(n-1)$ which we call the *hole stabilizer*. In Section 2.2, we describe how the Conway groupoid $\mathcal{C}(\mathcal{D})$ is completely determined by $\mathcal{L}_\infty(\mathcal{D})$, which explains the focus of the following theorem (and indeed the focus of Theorems D and E).

Theorem B. *Let $m \geqslant 3$ and let $\mathcal{D}^a$ and $\mathcal{D}^\varepsilon$ be as above. The following hold:*

(a) *Let ∞ be a point in $\mathcal{D}^\varepsilon$. Then $\mathcal{L}_\infty(\mathcal{D}^\varepsilon)$ coincides with a subgroup of $\mathrm{Sym}(\Omega^\varepsilon)$ isomorphic to $\mathrm{Sp}_{2m}(2)$ and $\pi_\infty(\mathcal{D}^\varepsilon)$ coincides with the stabilizer of ∞ inside $\mathcal{L}_\infty(\mathcal{D}^\varepsilon)$;*

(b) *Let ∞ be a point in $\mathcal{D}^a$. Then $\mathcal{L}_\infty(\mathcal{D}^a)$ coincides with a subgroup of $\mathrm{Sym}(V)$ isomorphic to $2^{2m}.\mathrm{Sp}_{2m}(2)$ and $\pi_\infty(\mathcal{D}^a)$ coincides with the stabilizer of ∞ inside $\mathcal{L}_\infty(\mathcal{D}^a)$.*

Recall that to any design $\mathcal{D}$ and prime $p > 0$ one may associate the code $C_{\mathbb{F}_p}(\mathcal{D})$, the $\mathbb{F}_p$-rowspan of the incidence matrix of $\mathcal{D}$. In [12], using GAP [11] we constructed examples of non-full Conway groupoids whose hole stabilizer is a primitive subgroup of $\mathrm{Sym}(n-1)$. In each case we also constructed $C_{\mathbb{F}_p}(\mathcal{D})$ for $p = 2$ or 3, and discovered that the code was *completely transitive* and, therefore, also *completely regular* (see Definitions 2.1 and 2.2 below).

The following result, Theorem C, asserts that the same is true of the $\mathbb{F}_2$-linear codes $C_{\mathbb{F}_2}(\mathcal{D}^\varepsilon)$ and $C_{\mathbb{F}_2}(\mathcal{D}^a)$ constructed using the designs considered in Theorem A. Theorem C also describes the covering radius and intersection array of these codes (see Definition 2.2). Recall that the function f_ε is defined at (1.1).

Theorem C. *Let $m \geqslant 3$ and let $\mathcal{D}^\varepsilon$ and $\mathcal{D}^a$ be as above. The following hold:*

(a) *$C_{\mathbb{F}_2}(\mathcal{D}^\varepsilon)$ is a completely transitive $[f_\varepsilon(m), f_\varepsilon(m) - (2m+1), 4]$ code with covering radius 3 and intersection array*

$$(f_\varepsilon(m), f_\varepsilon(m) - 1, f_\varepsilon(m) - 2f_\varepsilon(m-1); 1, 2f_\varepsilon(m-1), f_\varepsilon(m)).$$

(b) *$C_{\mathbb{F}_2}(\mathcal{D}^a)$ is a completely transitive $[2^{2m}, 2^{2m} - (2m+2), 4]$ code with covering radius 4 and intersection array*

$$(2^{2m}, 2^{2m} - 1, 2^{2m-1}, 1; 1, 2^{2m-1}, 2^{2m} - 1, 2^{2m}).$$

In fact, part (b) above is a consequence of a result of Borges, Rifà, and Zinoviev [3]. Completely regular and completely transitive codes have been studied extensively, and the existence and enumeration of such codes are open hard problems (see [5, 9, 20] and more recently [2, 3, 4, 14, 21, 22, 23]).

In [12, Question 8.4] we ask the following question. Suppose a Conway groupoid associated to a supersimple design $\mathcal{D}$ is not full and has a primitive hole stabilizer. Then does the incidence matrix of $\mathcal{D}$ generate a completely regular and/or uniformly packed $\mathbb{F}_p$-linear code for some prime $p > 0$? Since completely transitive codes are necessarily completely regular, by combining Theorems B and C we obtain an affirmative answer to this question for the designs $\mathcal{D}^\varepsilon$, $\mathcal{D}^a$.

The remainder of the paper is concerned with (abstract) Conway groupoids and our next main result classifies all Conway groupoids that satisfy a particular group-theoretic condition.

To understand its statement some comments are in order: note, first, that, for a supersimple design $\mathcal{D}$ with point set Ω, the hole stabilizer $G := \pi_\infty(\mathcal{D})$ is generated by elements of the form $[\infty, a, b, \infty]$ for $a, b \in \Omega \backslash \{\infty\}$ (see Section 2.1 for more discussion of $\pi_\infty(\mathcal{D})$). Note, second, that a *Boolean design* is a design whose point set is $(\mathbb{F}_2)^k$ for some $k > 1$ and whose blocks are given by the set of all affine subplanes of $(\mathbb{F}_2)^k$ (these designs are discussed at length in the earlier paper [12]). Note, finally, that the result is dependent on the Classification of Finite Simple Groups (CFSG) through its use of Theorem 6.2.

Theorem D. *Suppose that $\mathcal{D}$ is a supersimple $2-(n,4,\lambda)$ design, that ∞ is a point in $\mathcal{D}$, and write $\mathcal{L} := \mathcal{L}_\infty(\mathcal{D})$. Suppose, furthermore, that $[\infty, a, b, \infty] = 1$ whenever ∞ is collinear with $\{a, b\}$. Then one of the following is true:*

(1) *$\mathcal{D}$ is a Boolean design and $\mathcal{L} = (\mathbb{F}_2)^k$ for some $k > 1$;*
(2) *$\mathcal{D} = \mathbb{P}_3$ (the projective plane of order 3) and $\mathcal{L} = M_{13}$; or*
(3) *$\mathcal{L} = \mathrm{Alt}(n)$.*

Theorem D is a generalization of [12, Theorem B] (concerning designs associated with trivial hole stabilizer) as well as a generalization of the classification of Conway groupoids associated with supersimple $2-(n,4,1)$ designs (when $\lambda = 1$ the extra supposition is automatically satisfied).

Theorem D is closely connected to our final main result, Theorem E, below. Indeed we will use Theorem E (2) to prove Theorem D, and then will use Theorem D to prove Theorem E (4).

Theorem E. *Suppose that $\mathcal{D}$ is a supersimple $2-(n,4,\lambda)$ design, that ∞ is a point in $\mathcal{D}$, and that $\mathcal{L} := \mathcal{L}_\infty(\mathcal{D})$. Let $G := \pi_\infty(\mathcal{D})$ be the hole stabilizer of ∞, considered as a permutation group via its natural embedding in* $\mathrm{Sym}(n)$.

(1) *If $n > 4\lambda + 1$, then G is transitive;*
(2) *if $n > 9\lambda + 1$, then G is primitive;*
(3) *if $n > 144\lambda^2 + 120\lambda + 26$, then $\mathcal{L}$ contains* $\mathrm{Alt}(n)$*;*
(4) *If $n > 9\lambda^2 - 12\lambda + 5$, then one of the following holds:*
    (a) *$\mathcal{L}$ contains* $\mathrm{Alt}(n)$*;*
    (b) *$\lambda = 1$, $\mathcal{D} = \mathbb{P}_3$ (the projective plane of order 3), and $\mathcal{L} = M_{13}$.*

Note that only the fourth item of Theorem E is dependent on CFSG. Note too that if $\mathcal{L}$ contains $\mathrm{Alt}(n)$ (as in part (3) and (4) of the theorem), then

$$\mathcal{L} = \begin{cases} \mathrm{Alt}(n), & \text{if } \lambda \text{ is odd;} \\ \mathrm{Sym}(n), & \text{if } \lambda \text{ is even.} \end{cases}$$

1.2. **Classifying Conway groupoids.** Theorem E provides a powerful tool in the program to classify Conway groupoids for arbitrary λ and n. Such a classification was completed in [12] for $\lambda \leqslant 2$ and in Section 7.3 we make some remarks about the case $\lambda = 3$. What about the general case?

Firstly note that Theorem E has an immediate corollary:

Corollary 1.1. *Let λ be a positive integer. There are a finite number of (isomorphism classes of) groupoids that crop up as Conway groupoids associated with a supersimple $2-(n,4,\lambda)$ design.*

Corollary 1.1 makes an interesting companion to Theorem E which implies that if λ is allowed to vary, then there are an infinite number of (isomorphism classes) of groupoids that crop up as Conway groupoids.

One might naturally ask whether the bounds in Theorem E can be substantially improved as this would be an obvious aid to a classification. Unfortunately the relative dearth of examples of Conway groupoids makes this question difficult to answer: the only infinite families of non-full Conway groupoids which have been constructed to this point are those associated to the Boolean designs (for which $n = 2\lambda+2$ [12]) and the examples in Theorem C (for which $n < 5\lambda$). The parameters in these examples are a long way from the bounds given in Theorem E suggesting, perhaps, that there is plenty of room for improvement.

In a different direction we note that both Theorem D and Theorem E (4) suggest that the Conway groupoid associated to M_{13} is particularly special. Indeed we have another reason to think this might be the case.

Suppose that $\mathcal{C}$ is a Conway groupoid associated with a design $\mathcal{D}$, and suppose further that the hole stabilizer $\pi_\infty(\mathcal{D})$ is primitive. If $\mathcal{D}$ is not $\mathbb{P}_3$, the projective plane of order 3 and $\mathcal{C}$ is not full then in all examples known so far, $\mathcal{L}_\infty(\mathcal{D})$ is a transitive subgroup of $\mathrm{Sym}(n)$ with $\pi_\infty(\mathcal{D})$ the stabilizer of the point ∞ in $\mathcal{L}_\infty(\mathcal{D})$. Since, by supposition, $\pi_\infty(\mathcal{D})$ is primitive, this implies that $\mathcal{L}_\infty(\mathcal{D})$ is a *2-primitive* permutation group (i.e. a primitive group with a stabilizer primitive on its non-trivial orbit.) We conjecture that this behaviour is general.

Conjecture 1. *Suppose that $\mathcal{D}$ is a supersimple $2-(n,4,\lambda)$ design other than $\mathbb{P}_3$, that ∞ is a point in $\mathcal{D}$ and that the hole stabilizer $\pi_\infty(\mathcal{D})$ is primitive. Then $\mathcal{L}_\infty(\mathcal{D})$ coincides with a 2-primitive subgroup H of $\mathrm{Sym}(n)$ and $\pi_\infty(\mathcal{D})$ is equal to the stabilizer in $\mathcal{L}_\infty(\mathcal{D})$ of the point ∞.*

We remark that all 2-primitive permutation groups are known thanks to CFSG and the list is rather short (see [16] for some discussion). Thus this conjecture implies a very strong restriction on the structure of a Conway groupoid with primitive hole stabilizer and a proof would be a very significant step towards a classification.

One could push the conjecture a little further. Let us operate under the suppositions of Conjecture 1 and assume, moreover, that $\mathcal{L}_\infty(\mathcal{D})$ does not contain $\mathrm{Alt}(n)$. Now all known examples satisfy two further properties:

Firstly, the elements of $\mathcal{L}_\infty(\mathcal{D})$ are automorphisms of the design $\mathcal{D}$. Secondly, the group $\mathcal{L}_\infty(\mathcal{D})$ is a *3-transposition group* with associated class of transpositions coinciding with the set

$$\{[a,b] \mid a,b \in \Omega\}.$$

(Here Ω is the point set of $\mathcal{D}$; the elements $[a,b]$ are defined in Section 2.1.)

In forthcoming work the authors prove Conjecture 1 and the two additional statements just mentioned, provided the design $\mathcal{D}$ satisfies two mild combinatorial suppositions. It is expected that, by exploiting Fischer's famous theorem on 3-transposition groups, this will lead to a full classification of Conway groupoids in this restricted situtation [13].

1.3. **Structure of the paper.** The paper is structured as follows. Section 2 provides the necessary background from design theory, group theory and coding theory. In Section 3 we give a precise description of the action of $\mathrm{Sp}_{2m}(2)$ on quadratic forms, introduce the designs $\mathcal{D}^a$ and $\mathcal{D}^\varepsilon$ and prove Theorem A. The Conway groupoids $\mathcal{C}(\mathcal{D}^a)$ and $\mathcal{C}(\mathcal{D}^\varepsilon)$ are studied in Section 4 where we establish Theorem

B. In Section 5 we study the codes $C_{\mathbb{F}_2}(\mathcal{D}^a)$ and $C_{\mathbb{F}_2}(\mathcal{D}^\varepsilon)$ in detail and give a proof of Theorem C.

Sections 6 and 7 are devoted to the study of general Conway groupoids; in particular in Section 6 we prove Theorem D before proving Theorem E in Section 7. Section 7.3 contains a discussion of the classification of Conway groupoids with $\lambda = 3$.

2. Background

2.1. **Block designs and moves.** Recall that a *balanced incomplete block design* $(\Omega, \mathcal{B})$, or $t-(n,k,\lambda)$ design, is a finite set Ω of size n, together with a finite multiset $\mathcal{B}$ of subsets of Ω each of size k (called *lines*), such that any subset of Ω of size t is contained in exactly λ lines.

In what follows $\mathcal{D} = (\Omega, \mathcal{B})$ is a $2-(n,4,\lambda)$ design. We assume, moreover, that $\mathcal{D}$ is *supersimple*, i.e. any pair of lines intersect in at most two points. (Note that, in particular, $\mathcal{D}$ is *simple*, i.e. there are no repeated lines.)

Let a and b be distinct points in Ω. We define, first,

$$\overline{a,b} := \{x \in \Omega \,|\, \text{there exists } \ell \in \mathcal{B} \text{ such that } x, a, b, \in \ell\} \tag{2.1}$$

In particular, note that $a, b \in \overline{a,b}$.

Next, we define the *elementary move* associated with a and b: this is the permutation

$$[a,b] := (a,b)\prod_{i=1}^{\lambda}(a_i,b_i) \in \mathrm{Sym}(\Omega), \tag{2.2}$$

where $\{a,b,a_i,b_i\}$ is a line for each $1 \leqslant i \leqslant \lambda$. The fact that $\mathcal{D}$ is supersimple guarantees that the product (2.2) is well-defined. We note, moreover, that $[a,b] = [b,a]$ and that the set of points in Ω moved by the permutation $[a,b]$ (also called the *support* of $[a,b]$) is precisely the set $\overline{a,b}$.

A *move sequence* is a product of elementary moves

$$[a_0, a_1, \ldots, a_k] := [a_0,a_1]\cdot[a_1,a_2]\cdots[a_{k-1},a_k] \tag{2.3}$$

where $a_i \in \Omega$ for each $1 \leqslant i \leqslant k$. A move sequence $[a_0, a_1, \ldots, a_k]$ is called *closed* if $a_0 = a_k$.

Suppose that ∞ is a point in Ω. In this paper we will primarily study the following three sets for various designs $\mathcal{D}$:

$$\mathcal{L}(\mathcal{D}) := \{[a_0, a_1, \ldots, a_k] \mid k \in \mathbb{Z}^+,\ a_i \in \Omega \text{ for } 0 \leqslant i \leqslant k.\} \tag{2.4}$$

$$\mathcal{L}_\infty(\mathcal{D}) := \{[\infty, a_1, \ldots, a_k] \mid k \in \mathbb{Z}^+,\ a_i \in \Omega \text{ for } 1 \leqslant i \leqslant k.\} \tag{2.5}$$

$$\pi_\infty(\mathcal{D}) := \{[\infty, a_1, \ldots, a_{k-1}, \infty] \mid k \in \mathbb{Z}^+,\ a_i \in \Omega \text{ for } 1 \leqslant i \leqslant k-1.\} \tag{2.6}$$

Observe that $\pi_\infty(\mathcal{D}) \subseteq \mathcal{L}_\infty(\mathcal{D}) \subseteq \mathcal{L}(\mathcal{D})$.

The set $\pi_\infty(\mathcal{D})$ is called the *hole stabilizer*; it is precisely the set of all closed move sequences which start and end at ∞. It is an easy exercise to confirm that $\pi_\infty(\mathcal{D})$ is a group. We recall that $\pi_\infty(\mathcal{D})$ is generated by elements of the form $[\infty, a, b, \infty]$ for $a, b \in \Omega\backslash\{\infty\}$ [12, Lemma 3.1] and that if ∞_1 and ∞_2 are distinct elements of Ω, then $\pi_{\infty_1}(\mathcal{D}) \cong \pi_{\infty_2}(\mathcal{D})$ [12, Theorem A], since the hole stabilizers are conjugate subgroups of $\mathrm{Sym}(n)$.

By way of example, note that if $\mathcal{D} = \mathbb{P}_3$, the projective plane of order 3, then $\mathcal{L}_\infty(\mathcal{D})$ is equal to the set M_{13} originally defined by Conway. The group $\pi_\infty(\mathcal{D})$ is, then, a subset of Sym(12) isomorphic to the Mathieu group M_{12}.

2.2. **Conway groupoids.** Let $\mathcal{D} = (\Omega, \mathcal{B})$ be a supersimple $2-(n, 4, \lambda)$ design, as before. The *Conway groupoid* $\mathcal{C}(\mathcal{D})$ is the small category whose object set is Ω and such that, for $a, b \in \Omega$,

$$\mathrm{Mor}(a, b) := \{[a, a_1, \ldots, a_{k-1}, b] \mid a_{i-1}, a_i \in \Omega \text{ for } 1 \leqslant i \leqslant k-1.\}.$$

Observe that the set of all morphisms in the category $\mathcal{C}(\mathcal{D})$ is equal to the set $\mathcal{L}(\mathcal{D})$.

Two Conway groupoids $\mathcal{C}(\mathcal{D}_1)$ and $\mathcal{C}(\mathcal{D}_2)$ are *isomorphic* if they are isomorphic as categories, i.e. there exist two mutually inverse functors between $\mathcal{C}(\mathcal{D}_1)$ and $\mathcal{C}(\mathcal{D}_2)$. It is easy to check that this condition is equivalent to the condition that $\mathcal{D}_1$ and $\mathcal{D}_2$ contain the same number of points, n, and, moreover, that there exists $\phi \in \mathrm{Sym}(n)$ such that

$$\mathcal{L}(\mathcal{D}_2) = (\mathcal{L}(\mathcal{D}_1))^\phi := \{\phi^{-1} g \phi \mid g \in \mathcal{L}(\mathcal{D}_1)\}.$$

We return to the design $\mathcal{D}$ and fix a point ∞ in Ω. Clearly, for each $a, b \in \Omega$ and each $\sigma \in \mathrm{Mor}(a, b)$, there exist $\rho, \tau \in \mathcal{L}_\infty(\mathcal{D})$ such that $\sigma = \rho \cdot \tau^{-1}$. In particular the category $\mathcal{C}(\mathcal{D})$ is completely determined by $\mathcal{L}_\infty(\mathcal{D})$.

This straightforward observation underpins our work from here on: rather than studying the category $\mathcal{C}(\mathcal{D})$ directly, we prefer to study the set $\mathcal{L}_\infty(\mathcal{D})$. Indeed, in earlier literature on this subject these two objects have been treated as somewhat interchangeable: the label M_{13}, for instance, is sometimes used to refer to the set $\mathcal{L}_\infty(\mathbb{P}_3)$, sometimes to the groupoid $\mathcal{C}(\mathbb{P}_3)$. In what follows we will always treat M_{13} as a set and, indeed, we will have no need to study $\mathcal{C}(\mathcal{D})$ for any design at all.

2.3. **Permutation groups.** Let G be a finite group acting on a non-empty set Ω. The action is *transitive* if for any $x, y \in \Omega$ there exists $g \in G$ such that $x^g = y$ and *t-transitive* if the induced action on the set of all t-tuples of distinct elements of Ω is transitive for some $t > 0$.

Suppose that the action of G on Ω is transitive. A *system of imprimitivity* is a partition of Ω into ℓ subsets $\Delta_1, \Delta_2, \ldots, \Delta_\ell$ each of size k such that $1 < k, \ell < n$, and so that for all $i \in \{1, \ldots, \ell\}$ and all $g \in G$, there exists $j \in \{1, \ldots, \ell\}$ such that

$$\Delta_i^g = \Delta_j.$$

The sets Δ_i are called *blocks*. We say that G acts *imprimitively* if there exists a system of imprimitivity. If no such set exists then G acts *primitively* on Ω.

2.4. **Linear Codes.** Let C be a linear binary code of length n, i.e. C is a subspace of the vector space $(\mathbb{F}_2)^n$. Recall that elements of C are called *codewords*.

We define the *binary Hamming graph* $\Gamma = H(n, 2)$ to be the finite graph with vertex set $V(\Gamma) = (\mathbb{F}_2)^n$, such that an edge exists between two vertices if and only if they differ in precisely one entry. Observe that C is a subset of the vertex set of Γ.

For all pairs of vertices $\alpha, \beta \in V(\Gamma)$, the *Hamming distance* between α and β, denoted by $d(\alpha, \beta)$, is defined to be the number of entries in which the two vertices differ. We let $\Gamma_k(\alpha)$ denote the set of vertices in $H(n, 2)$ that are at distance k from α.

We are now able to define the *minimum distance, d, of C* to be the smallest distance between distinct codewords of C. For any $\gamma \in V(\Gamma)$, we define

$$d(\gamma, C) = \min\{d(\gamma, \beta) \,:\, \beta \in C\}$$

to be the *distance of γ from C*. The *covering radius of C*, which we denote by ρ, is the maximum distance that any vertex in $H(n,2)$ is from C. We let C_i denote the set of vertices that are at distance i from C; then $C_0 = C$ and $\{C, C_1, \dots, C_\rho\}$ forms a partition of $V(\Gamma)$ called the *distance partition of C*. For each i, the set C_i is a union of cosets of C, and we say that a coset that is a subset of C_i is *of weight i*.

The automorphism group of Γ, $\mathrm{Aut}(\Gamma)$, is the semi-direct product $B \rtimes L$ where $B \cong \mathrm{Sym}(2)^n$ and $L \cong \mathrm{Sym}(n)$, see [5, Theorem 9.2.1]. Let $g = (g_1, \dots, g_n) \in B$, $\sigma \in L$ and $\alpha = (\alpha_1, \dots, \alpha_n) \in V(\Gamma)$. Then g and σ act on α in the following way:

$$\alpha^g = (\alpha_1^{g_1}, \dots, \alpha_n^{g_n}), \quad \alpha^\sigma = (\alpha_{1\sigma^{-1}}, \dots, \alpha_{n\sigma^{-1}}). \tag{2.7}$$

The *automorphism group of C*, denoted by $\mathrm{Aut}(C)$, is the setwise stabiliser of C in $\mathrm{Aut}(\Gamma)$. In this paper, we construct a family of codes with the following symmetrical property.

Definition 2.1. Let C be a code with distance partition $\{C = C_0, C_1, \dots, C_\rho\}$. We say C is *X-completely transitive*, or simply *completely transitive*, if there exists $X \leqslant \mathrm{Aut}(\Gamma)$ such that C_i is an X-orbit for $i = 0, \dots, \rho$.

It is known that completely transitive codes are necessarily completely regular [14].

Definition 2.2. A binary code C with covering radius ρ is *completely regular* if for all $i \geqslant 0$, every vector $\alpha \in C_i$ has the same number c_i of neighbours in C_{i-1} and the same number b_i of neighbours in C_{i+1}; note that $c_0 = b_\rho = 0$. For such a code, define $(b_0, \dots, b_{\rho-1}; c_1, \dots, c_\rho)$ to be the *intersection array* of C.

Recall that the *dimension* of C is the dimension of C regarded as a vector space over $\mathbb{F}_2$. We say that C is an $[n,k,d]$ code if it has minimum distance d and dimension k. We will need the following result from [23].

Lemma 2.3. *Let C be a linear completely regular $[n,k,d]$ code with covering radius ρ and intersection array $(b_0, \dots, b_{\rho-1}; c_1, \dots, c_\rho)$. Let μ_i denote the number of cosets of C of weight i, where $i = 0, \dots, \rho$. Then the following equality holds:*

$$b_i \mu_i = c_{i+1} \mu_{i+1}, \ i = 0, \dots, \rho - 1.$$

3. The actions of $\mathrm{Sp}_{2m}(2)$ and $2^{2m}.\mathrm{Sp}_{2m}(2)$ on quadratic forms

The notation and terminology in this section will be based on that found in [10, Section 7.7]. We start with the standard construction for the action of $\mathrm{Sp}_{2m}(2)$ on quadratic forms. Let $m \geqslant 1$ be an integer and $V := \mathbb{F}_2^{2m}$ be a vector space equipped with the standard basis and consider the block matrices

$$e = \begin{pmatrix} 0_m & I_m \\ 0_m & 0_m \end{pmatrix}, \qquad f = \begin{pmatrix} 0_m & I_m \\ I_m & 0_m \end{pmatrix} = e + e^T.$$

We write elements of V as row matrices and, therefore, define $\varphi(u,v)$ to be the alternating bilinear form given by $\varphi(u,v) := ufv^T$. We let Ω be the set of all quadratic forms $\theta(u)$ with the property that

$$\varphi(u,v) = \theta(u+v) + \theta(u) + \theta(v),$$

i.e. Ω is the set of quadratic forms whose polarisation is equal to φ. Now we define $\theta_0(u) := ueu^T \in \Omega$, and by results in [10, Section 7.7], any other element of Ω is of the form

$$\theta_a(u) := \theta_0(u) + \varphi(u, a),$$

where a is a fixed element of V.

Recall that $\mathrm{Sp}_{2m}(2) := \{A \in \mathrm{GL}_{2m}(2) \mid AfA^T = f\}$ acts on Ω (on the right) via $\theta^x(u) := \theta(ux^{-1})$ for each $\theta \in \Omega$ and $x \in \mathrm{Sp}_{2m}(2)$. Recall ([10, Corollary 7.7A]) that the action of $\mathrm{Sp}_{2m}(2)$ on Ω splits into two distinct orbits

$$\Omega^0 := \{\theta_a \mid a \in V^0\}, \qquad \Omega^1 := \{\theta_a \mid a \in V^1\}$$

where

$$V^0 := \{a \in V \mid \theta_0(a) = 0\}, \qquad V^1 := \{a \in V \mid \theta_0(a) = 1\}.$$

Given the form φ and an element $c \in V$, we define the *transvection* t_c as follows:

$$u^{t_c} := u + \varphi(u, c)c, \text{ for all } u, c \in V.$$

Recall that the set of all transvections generates $\mathrm{Sp}_{2m}(2)$ (see, for instance, [24, Theorem 8.5]). The following result is [10, Lemma 7.7A].

Lemma 3.1. *The following hold:*

(i) *For all $a, c \in V$,*

$$\theta_a^{t_c} = \begin{cases} \theta_a, & \text{if } \theta_a(c) = 1; \\ \theta_{a+c}, & \text{if } \theta_a(c) = 0 \end{cases}$$

(ii) *For each $a, b \in V$ there is at most one $c \in V$ such that t_c maps θ_a onto θ_b. Such a c exists if and only if $\theta_0(a) = \theta_0(b)$ (and then $c = a + b$).*

As an immediate consequence, we obtain:

Lemma 3.2. *Let $\varepsilon \in \mathbb{F}_2$ and $\{v_1, \ldots, v_k\}$ a subset of V^ε for some odd integer $k > 0$. Then, for each $g \in \mathrm{Sp}_{2m}(2)$, we have*

$$\sum_{i=1}^{k} (\theta_{v_i})^g = \left(\theta_{\sum_{i=1}^{k} v_i}\right)^g. \tag{3.1}$$

Proof. We begin by considering the case where $g = 1$. Since k is odd,

$$\sum_{i=1}^{k} \theta_{v_i}(u) = \sum_{i=1}^{k} \theta_0(u) + \sum_{i=1}^{k} \varphi(u, v_i) = \theta_0(u) + \varphi(u, \sum_{i=1}^{k} v_i) = \theta_{\sum_{i=1}^{k} v_i}(u).$$

We now turn to the general case. Since the transvections generate $\mathrm{Sp}_{2m}(2)$, it suffices to consider the case $g = t_c$ for some $c \in V$. We calculate,

$$\begin{aligned}\sum_{i=1}^{k} \theta_{v_i}^{t_c}(u) &= \sum_{i=1}^{k} \theta_{v_i+(1+\theta_{v_i}(c))c}(u)\\ &= \sum_{i=1}^{k} \theta_0(u) + \varphi(u, v_i + (1+\theta_{v_i}(c))c)\\ &= \theta_0(u) + \varphi(u, \sum_{i=1}^{k} v_i + c + c\sum_{i=1}^{k} \theta_{v_i}(c))\\ &= \theta_0(u) + \varphi(u, \sum_{i=1}^{k} v_i + (1+\theta_{\sum_{i=1}^{k} v_i}(c))c) = \left(\theta_{\sum_{i=1}^{k} v_i}\right)^{t_c}(u).\end{aligned}$$

□

We now show how to decompose elements of V into a sum of elements in V^ε, which will prove useful in the sequel.

Lemma 3.3. *For each $v \in V$ and $\varepsilon \in \mathbb{F}_2$ there exist distinct $x, y \in V^\varepsilon$ such that $v = x + y$.*

Proof. We prove this in a series of cases. For $1 \leqslant i \leqslant 2m$, let e_i denote the i^{th} basis vector of V and, for each $v \in V$, let v_i denote the i^{th} coordinate of v. Let $y = x + v$ and $\delta := \theta_0(v)$.

(a) If $\delta = 0$, $\varepsilon = 0$ let $x := 0$.
(b) If $\delta = 0$, $\varepsilon = 1$ then
  (i) if $v_i = v_{i+m}$ for some $1 \leqslant i \leqslant m$, let $x := e_i + e_{i+m}$;
  (ii) if $v_i \neq v_{i+m}$ for all $1 \leqslant i \leqslant m$, fix any i, let j be such that either $v_{j-m} = 1$ or $v_{j+m} = 1$ and let $x := e_i + e_{i+m} + e_j$.
(c) If $\delta = 1$, $\varepsilon = 0$ let $1 \leqslant i \leqslant m$ be such that $v_i = v_{i+m} = 1$ and let $x := e_i$.
(d) If $\delta = 1$, $\varepsilon = 1$ let $1 \leqslant i \leqslant m$ be such that $v_i = v_{i+m} = 1$. Then
  (i) if $v_j = v_{j+m}$ for some $1 \leqslant j \leqslant m$ with $j \neq i$, let $x := e_j + e_{j+m} + e_i$;
  (ii) if $v_j \neq v_{j+m}$ for all $1 \leqslant j \leqslant m$ with $j \neq i$, let j be such that $v_{j-m} = 1$ or $v_{j+m} = 1$ and let $x := e_i + e_{i+m} + e_j$.

□

Corollary 3.4. *Let $v \in V^\varepsilon$. Then v can be written as the sum of three distinct elements of $V^{1-\varepsilon}$.*

Proof. By Lemma 3.3, $v = x + y$ for some $x, y \in V^{1-\varepsilon}$. Again, by Lemma 3.3, $y = y_1 + y_2$ for some $y_1, y_2 \in V^{1-\varepsilon}$ and so $v = x + y_1 + y_2$. Now if any of x, y_1, y_2 are equal, then $v \in V^{1-\varepsilon}$, which is a contradiction. □

3.1. **The action of $\mathrm{Sp}_{2m}(2)$ on 3-subsets.** In [10, Theorem 7.7A], the authors deduce that $\mathrm{Sp}_{2m}(2)$ acts 2-transitively on Ω^ε for $\varepsilon \in \mathbb{F}_2$. In fact, more is true:

Theorem 3.5. *Let $\varepsilon, \delta \in \mathbb{F}_2$ and $m \geqslant 3$. The action of $\mathrm{Sp}_{2m}(2)$ on 3-subsets of elements in Ω^ε splits into two orbits, $\mathcal{O}_0^\varepsilon$ and $\mathcal{O}_1^\varepsilon$, defined as follows:*

$$\mathcal{O}_\delta^\varepsilon := \Big\{ \{\theta_{v_1}, \theta_{v_2}, \theta_{v_3}\} \mid v_j \in V^\varepsilon, \theta_0(v_1 + v_2 + v_3) = \delta \Big\}.$$

Furthermore, for each $v \in V^\delta$, the sets

$$\Delta_v^\varepsilon := \left\{ \{\theta_{v_1}, \theta_{v_2}, \theta_{v_3}\} \in \mathcal{O}_\delta^\varepsilon \mid \sum_{i=1}^{3} v_i = v \right\}$$

form blocks of imprimitivity for the action of $\mathrm{Sp}_{2m}(2)$ *on* $\mathcal{O}_\delta^\varepsilon$.

We will prove Theorem 3.5 shortly. In order to do so we need a definition from [10]: Let $a \in V, \varepsilon \in \mathbb{F}_2$ and set

$$L(a, \varepsilon) := \{v \in V \mid \varphi(v, a) = \varepsilon\}.$$

Observe that $L(a, 0)$ is a subspace of V for all $a \in V$. Before the proof of Lemma 7.7B in [10], it is shown that

$$\dim \left(\bigcap_{i=1}^{k} L(a_i, 0) \right) = 2m - k,$$

whenever $\{a_1, \dots a_k\}$ are linearly independent. The following is a generalisation of [10, Lemma 7.7B].

Lemma 3.6. *Let $m \geqslant 4$ and let a, b, c be linearly independent vectors in V. For any $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \mathbb{F}_2$, θ_0 is not constant on*

$$L(a, \varepsilon_1) \cap L(b, \varepsilon_2) \cap L(c, \varepsilon_3).$$

Proof. By assumption, $U := L(a, 0) \cap L(b, 0) \cap L(c, 0)$ is a subspace of dimension $2m - 3 > 3$ in V, so there is $d \in U$ which is linearly independent of a, b and c. This means we may choose

$$w \in L(a, \varepsilon_1) \cap L(b, \varepsilon_2) \cap L(c, \varepsilon_3) \cap L(d, \varepsilon_4)$$

for any $\varepsilon_4 \in \mathbb{F}_2$. The fact that $d \in U$ implies that $w, w + d \in L(a, \varepsilon_1) \cap L(b, \varepsilon_2) \cap L(c, \varepsilon_3)$, so that on setting $\varepsilon_4 := \theta_0(d) + 1$, we have:

$$\theta_0(w + d) = \theta_0(w) + \theta_0(d) + \varphi(w, d) = \theta_0(w) + 1,$$

as needed. □

Proof of Theorem 3.5. Fix $\varepsilon, \delta \in \mathbb{F}_2$. We first prove that $\mathcal{O}_\delta^\varepsilon$, $\mathcal{O}_{1-\delta}^\varepsilon$ are the two distinct orbits of $\mathrm{Sp}_{2m}(2)$ on 3-subsets of Ω^ε. Let $\{\theta_{v_1}, \theta_{v_2}, \theta_{v_3}\} \in \mathcal{O}_\delta^\varepsilon$, so $\theta_{v_i} \in \Omega^\varepsilon$ for $i = 1, 2, 3$ and $\theta_{v_1+v_2+v_3} \in \Omega^\delta$. By Lemma 3.2, for $g \in \mathrm{Sp}_{2m}(2)$,

$$\theta_{v_1}^g + \theta_{v_1}^g + \theta_{v_1}^g = \theta_{v_1+v_2+v_3}^g.$$

Since Ω^δ is a $\mathrm{Sp}_{2m}(2)$-orbit, $\theta_{v_1+v_2+v_3}^g \in \Omega^\delta$, and hence $\{\theta_{v_1}^g, \theta_{v_1}^g, \theta_{v_1}^g\} \in \mathcal{O}_\delta^\varepsilon$. Thus both $\mathcal{O}_\delta^\varepsilon$, $\mathcal{O}_{1-\delta}^\varepsilon$ are fixed setwise by $\mathrm{Sp}_{2m}(2)$. When $m = 3$, a GAP [11] calculation verifies that each is in fact an $\mathrm{Sp}_{2m}(2)$-orbit. Thus we assume from now on that $m \geqslant 4$.

Since $\mathrm{Sp}_{2m}(2)$ acts 2-transitively on Ω^ε, it is sufficient to prove that whenever $a, b, c, d \in V^\varepsilon$, there is an element x of $\mathrm{Sp}_{2m}(2)$ which fixes θ_c, θ_d but maps θ_a to θ_b if and only if $\theta_0(a + c + d) = \theta_0(b + c + d)$. (Recall that $\{\theta_a, \theta_c, \theta_d\}$ and $\{\theta_b, \theta_c, \theta_d\}$ are both elements in $\mathcal{O}_\delta^\varepsilon$, or both elements in $\mathcal{O}_{1-\delta}^\varepsilon$, if and only if $\theta_0(a + c + d) = \theta_0(b + c + d)$.)

In order to prove this fact, we will show that there is $w \in V^\varepsilon$ such that

$$\theta_c(a + w) = \theta_c(b + w) = \theta_d(a + w) = \theta_d(b + w) = 1 \tag{3.2}$$

if and only if $\theta_0(a+c+d) = \theta_0(b+c+d)$. Note that, since $w \in V^\varepsilon$, we easily deduce that

$$\theta_a(a+w) = \theta_w(b+w) = 0.$$

This, along with (3.2) and Lemma 3.1, implies that we may take $x = t_{a+w} \cdot t_{b+w}$ and we are done.

Thus it remains to show that there is $w \in V^\varepsilon$ satisfying (3.2). One easily checks that (3.2) is equivalent to

$$\begin{aligned}\varphi(w, a+c) &= 1 + \varphi(a,c);\\ \varphi(w, a+d) &= 1 + \varphi(a,d);\\ \varphi(w, b+c) &= 1 + \varphi(b,c);\\ \varphi(w, b+d) &= 1 + \varphi(b,d).\end{aligned}$$

Since the vectors $\{a+c, b+c, a+d\}$ are linearly independent, Lemma 3.6 implies that θ_0 is not constant on

$$L(a+c, 1+\varphi(a,c)) \cap L(b+c, 1+\varphi(b,c)) \cap L(a+d, 1+\varphi(a,d))$$

(notice that this assertion holds even if $d = a+b+c$ by [10, Lemma 7.7B].) Thus whatever value ε takes, there exists $w \in V^\varepsilon$ satisfying the conditions in (3.2) if and only if $\varphi(w, b+d) = 1 + \varphi(b,d)$ holds above. But $\theta_0(a+c+d) = \theta_0(b+c+d)$ if and only if $\varphi(b,c) + \varphi(b,d) = \varphi(a,c) + \varphi(a,d)$ which is if and only if

$$\varphi(w,b+d) = \varphi(w,b) + \varphi(w,d) = \varphi(b,c) + \varphi(w,c) + \varphi(a,d) + \varphi(w,a)$$

$$= \varphi(b,d) + \varphi(a,c) + \varphi(w,c) + \varphi(w,a) = 1 + \varphi(b,d),$$

as required. This proves the first assertion in Theorem 3.5.

It remains to prove the last statement. Let t_c be a transvection in $\mathrm{Sp}_{2m}(2)$, and suppose that $(\Delta_v^\varepsilon)^{t_c} \cap \Delta_v^\varepsilon \neq \emptyset$. Then there exist two elements of Δ_v^ε such that

$$\{\theta_{v_1}, \theta_{v_2}, \theta_{v_3}\} = \{\theta_{x_1}^{t_c}, \theta_{x_2}^{t_c}, \theta_{x_3}^{t_c}\}.$$

We deduce from Lemma 3.2 that

$$\theta_v = \theta_{v_1+v_2+v_3} = \theta_{v_1} + \theta_{v_2} + \theta_{v_3} = \theta_{x_1}^{t_c} + \theta_{x_2}^{t_c} + \theta_{x_3}^{t_c} = \theta_{x_1+x_2+x_3}^{t_c} = \theta_v^{t_c},$$

in particular we have that $\theta_v(c) = 1$. One can now deduce that $\{\theta_{y_1}, \theta_{y_2}, \theta_{y_3}\}^{t_c} \in \Delta_v^\varepsilon$ for all $\{\theta_{y_1}, \theta_{y_2}, \theta_{y_3}\} \in \Delta_v^\varepsilon$, that is $(\Delta_v^\varepsilon)^{t_c} = \Delta_v^\varepsilon$. Since $\mathrm{Sp}_{2m}(2)$ is generated by transvections, and because it acts transitively on $\mathcal{O}_\delta^\varepsilon$, the final statement now follows. □

3.2. **The action of $2^{2m}.\mathrm{Sp}_{2m}(2)$ on 3-subsets.** We next consider an analogous situation for the affine group $2^{2m}.\mathrm{Sp}_{2m}(2)$ whose elements may be identified with pairs (v,g) with $v \in (\mathbb{F}_2)^{2m}$ and $g \in \mathrm{Sp}_{2m}(2)$, and the action on V is given by

$$u^{(v,g)} = u^g + v^g \ \ \forall u \in V. \tag{3.3}$$

Theorem 3.7. *Let $m \geqslant 3$. The action of $2^{2m}.\mathrm{Sp}_{2m}(2)$ on 3-subsets of elements in V splits into two orbits, $\mathcal{O}_0$ and $\mathcal{O}_1$, defined as follows:*

$$\mathcal{O}_\delta := \{\{v_1, v_2, v_3\} \mid v_i \in V, \varphi(v_1,v_2) + \varphi(v_1,v_3) + \varphi(v_2,v_3) = \delta\}.$$

Proof. When $m = 2, 3$ we verify all assertions via a GAP [11] computation, so we assume from now on that $m \geqslant 4$. Let $\{v_1, v_2, v_3\} \in \mathcal{O}_\delta$. Then a straightforward calculation shows that

$$\sum_{\substack{\mathrm{i,j=1}\\ \mathrm{i<j}}}^{3} \varphi(v_i^{(v,g)}, v_j^{(v,g)}) = \sum_{\substack{\mathrm{i,j=1}\\ \mathrm{i<j}}}^{3} \varphi(v_i^g, v_j^g),$$

and because $\mathrm{Sp}_{2m}(2)$ preserves φ, the right hand side of the above equation is equal to δ. Hence $\mathcal{O}_\delta$ is fixed setwise by $2^{2m}.\mathrm{Sp}_{2m}(2)$.

As is well-known, $2^{2m}.\mathrm{Sp}_{2m}(2)$ acts 2-transitively on V, so it suffices to show that for each $a, b, c, d \in V$ there is an element of $2^{2m}.\mathrm{Sp}_{2m}(2)$ which fixes c, d and maps a to b if and only if

$$\varphi(a, c) + \varphi(a, d) = \varphi(b, c) + \varphi(b, d). \tag{3.4}$$

As in the proof of Theorem 3.5 there exists $w \in V$ such that

$$\varphi(w, a + c) = 1 + \varphi(a, c);$$
$$\varphi(w, a + d) = 1 + \varphi(a, d);$$
$$\varphi(w, b + c) = 1 + \varphi(b, c).$$

Summing up the left hand sides of these equations and using (3.4) we see that $\varphi(w, b+d) = 1+\varphi(b, d)$. It is now easy to verify that the element $g \cdot h \in 2^{2m}.\mathrm{Sp}_{2m}(2)$ has the required property with

$$g := (w^{t_a} + a^{t_w}, t_{a+w}) \text{ and } h := (w^{t_b} + b^{t_w}, t_{b+w}).$$

□

3.3. **Construction of $\mathcal{D}^\varepsilon$.** For $\varepsilon \in \mathbb{F}_2$, it follows from Lemma 3.2 that we can describe $\mathcal{B}^\varepsilon$ from Theorem A as:

$$\mathcal{B}^\varepsilon := \{\{\theta_a, \theta_b, \theta_c, \theta_{a+b+c}\} \mid \{\theta_a, \theta_b, \theta_c\} \in \mathcal{O}_\varepsilon^\varepsilon\}.$$

Lemma 3.8. *$\mathcal{D}^\varepsilon := (\Omega^\varepsilon, \mathcal{B}^\varepsilon)$ is a supersimple $2 - (|\Omega^\varepsilon|, 4, \lambda^\varepsilon)$ design for some $\lambda^\varepsilon > 0$.*

Proof. Clearly $\mathcal{B}^\varepsilon$ contains no repeated lines (by definition). Moreover, given any $\ell \in \mathcal{B}^\varepsilon$, any three points in ℓ uniquely determine the fourth, so the intersection of any two lines has size at most 2. As $\mathcal{O}_\varepsilon^\varepsilon$ is an $\mathrm{Sp}_{2m}(2)$-orbit, we deduce from Lemma 3.2 that $\mathcal{B}^\varepsilon$ is a $\mathrm{Sp}_{2m}(2)$-orbit on the 4-subsets of Ω^ε. Since $\mathrm{Sp}_{2m}(2)$ acts 2-transitively on Ω^ε, $\mathcal{D}^\varepsilon := (\Omega^\varepsilon, \mathcal{B}^\varepsilon)$ is a $2 - (|\Omega^\varepsilon|, 4, \lambda^\varepsilon)$ design for some $\lambda^\varepsilon > 0$ by [12, Lemma 4.3]. □

For the design $\mathcal{D}^\varepsilon$, it remains to calculate the values of $|\Omega^\varepsilon|$ and λ^ε. It is well known that $n^\varepsilon := |\Omega^\varepsilon| = |V^\varepsilon| = 2^{m-1}(2^m + (-1)^\varepsilon)$. One proof of this comes from a (probably well known) inductive construction for V^ε, which we now describe.

For $k > 0$ let V_k denote the $\mathbb{F}_2$-vector space of dimension $2k$, and as before, $V_k^\varepsilon = \{v \in V_k \mid \theta_0(v) = \varepsilon\}$ where θ_0 is defined over the appropriate dimension. For each $x, y \in \mathbb{F}_2$, $k > 0$ and $v = (v_1, v_2) \in V_k$ (here each v_i is an $\mathbb{F}_2$-vector of length k), let $v_{xy} = (x, v_1, y, v_2) \in V_{k+1}$. Moreover, let $(V_k^\varepsilon)^{xy} := \{v_{xy} \mid v \in V_k^\varepsilon\} \subseteq V_{k+1}$.

Lemma 3.9. *For each $\varepsilon \in \mathbb{F}_2$,*

$$V_{k+1}^\varepsilon = (V_k^\varepsilon)^{00} \cup (V_k^\varepsilon)^{01} \cup (V_k^\varepsilon)^{10} \cup (V_k^{1-\varepsilon})^{11}.$$

In particular, $|V_{k+1}^\varepsilon| = 3|V_k^\varepsilon| + |V_k^{1-\varepsilon}|$ and $|V_m^\varepsilon| = 2^{m-1}(2^m + (-1)^\varepsilon)$.

Proof. Clearly each of $(V_k^\varepsilon)^{00}$, $(V_k^\varepsilon)^{01}$, $(V_k^\varepsilon)^{10}$ and $(V_k^{1-\varepsilon})^{11}$ is contained in V_{k+1}^ε. Conversely any element of V_{k+1}^ε must lie in one of these sets. Thus, since these sets are pairwise disjoint, $|V_{k+1}^\varepsilon| = 3|V_k^\varepsilon| + |V_k^{1-\varepsilon}|$. Obtaining an explicit formula for $|V_k^\varepsilon|$ is now safely left as an exercise. □

Lemma 3.10. *Let λ^ε be the number of lines that contain any pair of points in the design $\mathcal{D}^\varepsilon$. Then*

$$\lambda^\varepsilon = 2^{m-2}(2^{m-1} + (-1)^\varepsilon) - 1.$$

Proof. Let $\theta_w, \theta_z \in \Omega^\varepsilon$, and recall from (2.1) the definition of $\overline{\theta_w, \theta_z}$. Then $\theta_v \in \overline{\theta_w, \theta_z}$ if and only if $\theta_0(w + z + v) = \varepsilon$. As $\mathcal{D}^\varepsilon$ is supersimple, $2 + 2\lambda^\varepsilon = |\overline{\theta_w, \theta_z}|$, and so

$$2 + 2\lambda^\varepsilon = |\{v \in V_m^\varepsilon \mid \theta_0(w + z + v) = \varepsilon\}|.$$

Since $\mathrm{Sp}_{2m}(2)$ acts 2-transitively on Ω^ε, we can assume that $w = 0$ and $z = e_1$, or $w = e_1 + e_2 + e_{m+2}$ and $z = e_2 + e_{m+2}$ for $\varepsilon = 0$ or 1 respectively. In particular, we can assume that $w + z = e_1$. Now, for $v \in V_m^\varepsilon$, $\theta_0(e_1 + v) = \varepsilon$ if and only if $v_{m+1} = 0$. Hence, by Lemma 3.9,

$$\{v \in V_m^\varepsilon \mid \theta_0(w + z + v) = \varepsilon\} = (V_{m-1}^\varepsilon)^{00} \cup (V_{m-1}^\varepsilon)^{10},$$

and so $2 + 2\lambda^\varepsilon = 2|V_{m-1}^\varepsilon| = 2^{m-1}(2^{m-1} + (-1)^\varepsilon)$. Rearranging this gives the result. □

3.4. **Construction of $\mathcal{D}^a$.** Define $\mathcal{B}^a$ as in the statement of Theorem A:

$$\mathcal{B}^a := \{\{v_1, v_2, v_3, v_1 + v_2 + v_3\} \mid v_i \in V, \sum_{i=1}^3 \theta_0(v_i) = \theta_0\left(\sum_{i=1}^3 v_i\right)\}.$$

Lemma 3.11. *$\mathcal{D}^a := (V, \mathcal{B}^a)$ is a supersimple $2 - (2^{2m}, 4, 2^{2m-2} - 1)$ design.*

Proof. $\mathcal{B}^a$ contains no repeated lines (by definition) and for each $\ell \in \mathcal{B}^a$, any three points in ℓ uniquely determine the fourth, so the intersection of any two lines has size at most 2. Now by Theorem 3.7, $\mathcal{O}_0$ is a $2^{2m}.\mathrm{Sp}_{2m}(2)$-orbit. Also for each $(v, g) \in 2^{2m}.\mathrm{Sp}_{2m}(2)$,

$$(v_1 + v_2 + v_3)^{(v,g)} = (v_1 + v_2 + v_3)^g + v^g = \sum_{i=1}^3 (v_i^g + v^g) = \sum_{i=1}^3 v_i^{(v,g)},$$

and we deduce that $\mathcal{B}^a$ is a $2^{2m}.\mathrm{Sp}_{2m}(2)$-orbit on the 4-subsets of V. Since $2^{2m}.\mathrm{Sp}_{2m}(2)$ acts 2-transitively on V, $\mathcal{D}^a := (V, \mathcal{B}^a)$ is a $2 - (|V|, 4, \lambda)$ design for some $\lambda > 0$, and it remains to calculate λ. Now, for each $x, y \in V$, by definition,

$$2\lambda + 2 = |\{z \in V \mid \varphi(x, y) + \varphi(x, z) + \varphi(y, z) = 0\}|.$$

Using the 2-transitivity of $2^{2m}.\mathrm{Sp}_{2m}(2)$ again, we may assume that $x = 0$ and $y = e_1 = (1, 0, \ldots, 0)$. Hence $2\lambda + 2 = |\{z \in V \mid \varphi(e_1, z) = 0\}|$ which has order 2^{2m-1}. The result follows. □

Proof of Theorem A. Theorem A follows as an immediate consequence of Lemmas 3.8, 3.9, 3.10 and 3.11. □

4. Infinite families of Conway groupoids

In this section, our goal is a description of the Conway groupoids $\mathcal{C}(\mathcal{D}^\varepsilon)$ and $\mathcal{C}(\mathcal{D}^a)$. Taken together, the results of this section yield a proof of Theorem B. First recall the notation $[x, y]$ of Section 2.1 for a pair $\{x, y\}$ of points in a supersimple $2-(n, 4, \lambda)$ design.

Lemma 4.1. *The following hold:*

(a) *For each $x_0, y_0 \in V^\varepsilon$, the action of $t_{x_0+y_0}$ on Ω^ε induces the permutation $[\theta_{x_0}, \theta_{y_0}]$ defined by $\mathcal{B}^\varepsilon$.*
(b) *For each $x_0, y_0 \in V$, the action of $(y_0^{t_{x_0}} + x_0^{t_{y_0}}, t_{x_0+y_0})$ on V induces the permutation $[x_0, y_0]$ defined by $\mathcal{B}^a$.*

Proof. To prove (a), our goal is to show that $t_{x_0+y_0}$ induces the permutation

$$\prod_{i=0}^{\lambda^\varepsilon} (\theta_{x_i}, \theta_{y_i}),$$

where $\{\theta_{x_0}, \theta_{y_0}, \theta_{x_i}, \theta_{y_i}\}$ are the lines in $\mathcal{B}^\varepsilon$ containing $\{\theta_{x_0}, \theta_{y_0}\}$ for $1 \leqslant i \leqslant \lambda^\varepsilon$. Note that $\theta_0(x_0 + y_0 + x_i) = \varepsilon$ and $x_i + y_i = x_0 + y_0$, so writing $c := x_0 + y_0$ we have $\theta_{x_i}(c) = \theta_{y_i}(c) = 0$. Hence by Lemma 3.1,

$$\theta_{x_i}^{t_c} = \theta_{x_i+c} = \theta_{x_i+x_0+y_0} = \theta_{x_i+x_i+y_i} = \theta_{y_i},$$

and similarly $\theta_{y_i}^{t_c} = x_i$.

Finally, if $z \in V^\varepsilon$ is such that $\theta_0(c + z) = 1 - \varepsilon$ then

$$\theta_z(c) = \theta_0(c) + \varphi(c, z) = \theta_0(c + z) + \theta_0(z) = 1 - \varepsilon + \varepsilon = 1,$$

so that $\theta_z^{t_c} = \theta_z$. This completes the proof of (a).

We next prove (b). Recall from (3.3) that we regard elements of $2^{2m}.\mathrm{Sp}_{2m}(2)$ as ordered pairs (v, g), so that the action of $2^{2m}.\mathrm{Sp}_{2m}(2)$ on V is described by

$$x^{(v,g)} := x^g + v^g$$

for each $x \in V$. We need to show that $h := (y_0^{t_{x_0}} + x_0^{t_{y_0}}, t_{x_0+y_0})$ induces the permutation

$$\prod_{i=0}^{\lambda} (x_i, y_i)$$

where $\{x_0, y_0, x_i, y_i\}$ are the lines in $\mathcal{B}^a$ containing $\{x_0, y_0\}$ for $1 \leqslant i \leqslant \lambda$. Observe that

$$y_0^{t_{x_0}} + x_0^{t_{y_0}} = (1 + \varphi(x_0, y_0))(x_0 + y_0),$$

so that

$$\begin{aligned} x_0^h &= x_0^{t_{x_0+y_0}} + (1 + \varphi(x_0, y_0))(x_0 + y_0) \\ &= x_0 + \varphi(x_0, x_0 + y_0)(x_0 + y_0) + (1 + \varphi(x_0, y_0))(x_0 + y_0) \\ &= x_0 + x_0 + y_0 = y_0, \end{aligned}$$

and similarly for y_0. Next, for any $1 \leqslant i \leqslant \lambda$, we have that $\varphi(x_i, x_0+y_0) = \varphi(x_0, y_0)$, so that

$$\begin{aligned} x_i^h &= x_i^{t_{x_0+y_0}} + (1+\varphi(x_0,y_0))(x_0+y_0) \\ &= x_i + \varphi(x_i, x_0+y_0)(x_0+y_0) + (1+\varphi(x_0,y_0))(x_0+y_0) \\ &= x_i + x_0 + y_0 = y_i \end{aligned}$$

Lastly, if $r \notin \overline{x_0, y_0}$ then $\varphi(r, x_0+y_0) = \varphi(x_0,y_0)+1$, and a similar calculation shows that $r^h = r$. This completes the proof. □

Lemma 4.2. *Let $u, v, w \in V$ be such that*

$$\varphi(u,v) + \varphi(u,w) + \varphi(v,w) = 1. \tag{4.1}$$

The following hold:

(a) $t_{u+v}^{t_{v+w}} = t_{u+w}$.
(b) $x^y = z$, *where*

$$x := (v^{t_u} + u^{t_v}, t_{u+v}) \quad y := (w^{t_v} + v^{t_w}, t_{v+w}) \quad z := (w^{t_u} + u^{t_w}, t_{u+w})$$

Proof. To prove (a), we note, by [10, p.246], that $u^{t_v} = u + \varphi(u,v)v$ for all $u, v \in V$, and $x^{-1}t_v x = t_{vx}$ for all $x \in \mathrm{Sp}_{2m}(2)$. Using (4.1), it is straightforward to show that $(u+v)^{t_{v+w}} = u+w$, from which the result now follows.

It remains to prove that $x^y = z$, as in the statement of the lemma. If $(a,b),(c,d) \in 2^{2m}.\mathrm{Sp}_{2m}(2)$, by the usual multiplication rule for the semi-direct product we have:

$$(a,b)^{(c,d)} = ((c^{-1})^d + a^d + c^{(d^{-1}b)^{-1}}, b^d).$$

We will apply in the case where

$$a = v^{t_u} + u^{t_v}, \qquad b = t_{u+v}, \qquad c = w^{t_v} + v^{t_w}, \qquad d = t_{v+w}.$$

It thus suffices to prove that $(c^{-1})^d + a^d + c^{(d^{-1}b)^{-1}} = w^{t_u} + u^{t_w}$.

Note that for each $\{i,j,k\} = \{u,v,w\}$,

$$(i+k)^{t_{i+j}} = j+k.$$

Using this we obtain the following two equations:

$$\begin{aligned} a^d &= (\varphi(u,v)+1)(u+v)^{t_{v+w}} = (\varphi(u,v)+1)(u+w), \\ c^{(d^{-1}b)^{-1}} &= c^{bd} = (\varphi(w,v)+1)((v+w)^{t_{u+v}t_{v+w}}) = (\varphi(w,v)+1)(v+u)). \end{aligned}$$

Noting also that $(c^{-1})^d = c^d = c = (\varphi(v,w)+1)(v+w)$, we conclude

$$c + a^d + c^{bd} = (\varphi(w,v)+\varphi(u,v))(u+w) = (\varphi(u,w)+1)(u+w) = w^{t_u} + u^{t_w}.$$

This completes the proof. □

For the remainder of this section we identify, in both cases, the points of the respective design with vectors in V, allowing us to amalgamate arguments. We now combine Lemmas 4.1 and 4.2 to obtain the following corollary:

Corollary 4.3. *Let ∞, a, b be a triple of points in $\mathcal{D}^\varepsilon$ or $\mathcal{D}^a$ such that $\infty \notin \overline{a,b}$. Then*

$$[\infty, a]^{[a,b]} = [\infty, b].$$

Consequently, $[\infty, a, b, \infty] = [a, b]$.

Proof. In both cases, $\infty \notin \overline{a,b}$ implies that

$$\varphi(\infty, a) + \varphi(\infty, b) + \varphi(a, b) = 1.$$

Hence by Lemmas 4.1 and 4.2, we have that $[\infty, a]^{[a,b]} = [\infty, b]$. Now two applications of Lemma 4.2 yield

$$\begin{aligned}[\infty, a, b, \infty] &= [\infty, a][a, b][b, \infty] = [\infty, a][a, b][\infty, a][\infty, a][b, \infty] \\ &= [\infty, b][\infty, a][b, \infty] = [a, b],\end{aligned}$$

as required. □

For the designs $\mathcal{D}^\varepsilon$ (respectively $\mathcal{D}^a$) recall that $\mathcal{L}(\mathcal{D}^\varepsilon)$ (respectively $\mathcal{L}(\mathcal{D}^a)$) denote the set of *all* move sequences. We will apply Corollary 4.3 to show that the permutation induced by a move sequence in $\mathcal{L}(\mathcal{D}^\varepsilon)$ or $\mathcal{L}(\mathcal{D}^a)$ can be generated with a move sequence which starts with an element of our choosing:

Lemma 4.4. *Let $\mathcal{L}$ be either of the sets $\mathcal{L}(\mathcal{D}^\varepsilon)$ or $\mathcal{L}(\mathcal{D}^a)$. For any $g \in \mathcal{L}$ and any point ∞, there exist $l > 0$ and a set of points $\{b_1, \ldots, b_l\}$ such that $g = [\infty, b_1, b_2 \ldots, b_l]$.*

Proof. We prove this by induction on the length k of an expression for an element $g := [a_1, a_2, \ldots, a_k] \in \mathcal{L}$. If $k = 2$ then there are two cases to consider. If $\infty \in \overline{a_1, a_2}$ then $[a_1, a_2] = [\infty, \infty + a_1 + a_2]$, otherwise $[a_1, a_2] = [\infty, a_1, a_2, \infty]$ by Corollary 4.3. Now assume that $k > 2$. If $\infty \in \overline{a_1, a_2}$ then by induction there exist $l > 0$ and $b_i \in \Omega$ for $1 \leqslant i \leqslant l$ such that $[a_2, \ldots, a_k] = [\infty + a_1 + a_2, b_1, \ldots, b_l]$ and hence $g = [\infty, \infty + a_1 + a_2, b_1, \ldots, b_l]$. If $\infty \notin \overline{a_1, a_2}$ then there exist $l > 0$ and $b_i \in \Omega$ for $1 \leqslant i \leqslant l$ such that $[a_2, \ldots, a_k] = [\infty, b_1, \ldots, b_l]$ so that $g = [\infty, a_1, a_2, \infty, b_1, \ldots, b_l]$. The result follows. □

Corollary 4.5. *Let $\mathcal{L}$ be either of the sets $\mathcal{L}(\mathcal{D}^\varepsilon)$ or $\mathcal{L}(\mathcal{D}^a)$. Then $\mathcal{L}$ is a group. Furthermore, for each point ∞, we have $\mathcal{L} = \mathcal{L}_\infty(\mathcal{D})$.*

Proof. $\mathcal{L}$ clearly contains the trivial move sequence and $[a_1, a_2, \ldots, a_r]^{-1} = [a_r, a_{r-1}, \ldots, a_1]$ for each $[a_1, a_2, \ldots, a_r] \in \mathcal{L}$. It remains to show that $\mathcal{L}$ is closed under composition.

For $1 \leqslant i \leqslant k$ and $1 \leqslant j \leqslant l$ let a_i, b_j be points and write $g := [a_1, \ldots, a_k]$ and $h := [b_1, \ldots, b_l]$. By Lemma 4.4, there exist $s > 0$ and points $c_1, \ldots c_s$ such that $[b_1, \ldots, b_l] = [a_k, c_1, \ldots, c_s]$ so we have $g \cdot h = [a_1, \ldots, a_k, c_1, \ldots, c_s] \in \mathcal{L}$, as required.

The last statement follows immediately from Lemma 4.4. □

Proof of Theorem B. First note that, by Corollary 4.5, $\mathcal{L}(\mathcal{D}^\varepsilon)$ and $\mathcal{L}(\mathcal{D}^a)$ are both groups. In both cases, this group is generated by all elementary move sequences $[a, b]$. In this first case, $[a, b] = t_{a+b}$ for all $a, b \in \Omega^\varepsilon$ (Lemma 4.1), and since every $v \in V$ can be written as the sum of two elements in V^ε (Lemma 3.3), it follows that

$$\mathcal{L}(\mathcal{D}^\varepsilon) = \langle t_{a+b} \,|\, a, b \in V^\varepsilon \rangle = \langle t_v \,|\, v \in V \rangle \cong \mathrm{Sp}_{2m}(2).$$

In the second case, $[a, b] = (a^{t_b} + b^{t_a}, t_{a+b})$, by Lemma 4.1, and so $\mathcal{L}(\mathcal{D}^a) \leqslant 2^{2m}.\mathrm{Sp}_{2m}(2)$. Now, it is straightforward to show that for every $0 \neq a \in V$, there exists $x_a \in V$ such that $\varphi(x_a, a) = 1$. One then calculates that $[x_a, x_a + a] = (0, t_a)$ for all $0 \neq a \in V$, so $\mathrm{Sp}_{2m}(2) \cong \langle [x_v, x_v + v] \,|\, v \in V \rangle \leqslant \mathcal{L}(\mathcal{D}^a)$. To get the

translations of the affine group, we observe that $[0,a] = (a, t_a)$ for all $a \in V$, so $[0,a][x_a, x_a + a] = (a, 1)$. Thus

$$\mathcal{L}(\mathcal{D}^a) \cong 2^{2m}.\,\mathrm{Sp}_{2m}(2).$$

Now let $\mathcal{L}$ denote $\mathcal{L}(\mathcal{D}^\varepsilon)$ (respectively $\mathcal{L}(\mathcal{D}^a)$) and π denote $\pi_\infty(\mathcal{D}^\varepsilon)$ (respectively $\pi_\infty(\mathcal{D}^a)$). By [12, Lemma 3.1], $|\mathcal{L}| = n \cdot |\pi|$ where n is the number of points in the associated design, and since $\pi \subseteq \mathrm{stab}_{\mathcal{L}}(\infty)$ we must have an equality $\pi = \mathrm{stab}_{\mathcal{L}}(\infty)$. This completes the proof. □

5. Infinite Families of Completely Transitive Codes

This section is concerned with the $\mathbb{F}_2$-linear codes $C^\varepsilon := C_{\mathbb{F}_2}(\mathcal{D}^\varepsilon)$ and $C^a := C_{\mathbb{F}_2}(\mathcal{D}^a)$ associated respectively to the incidence matrices of the designs $\mathcal{D}^\varepsilon$ and $\mathcal{D}^a$ of Theorem A. (Recall that $C_{\mathbb{F}_2}(\mathcal{E})$ is simply the $\mathbb{F}_2$-rowspan of the incidence matrix of a design $\mathcal{E}$.) We first introduce some notation which will allow us to describe elements of C^ε and C^a succinctly. For $\varepsilon \in \mathbb{F}_2$, let W^ε be the $|\Omega^\varepsilon|$-dimensional vector space over $\mathbb{F}_2$ with entries indexed by Ω^ε and W^a be the $|\Omega|$-dimensional vector space over $\mathbb{F}_2$ with entries indexed by V. Therefore, each element $\alpha_{\mathcal{S}}$ of W^ε or W^a can be uniquely identified with a subset $\mathcal{S}$ of Ω^ε or V, that is, $\alpha_{\mathcal{S}}$ is the characteristic vector of $\mathcal{S}$. Thus, we note that $\mathrm{supp}(\alpha_{\mathcal{S}}) = \mathcal{S}$ ($\mathrm{supp}(v)$ denotes the *support* of a vector v, that is, the set of non-zero entries of v). Using this notation

$$C^\varepsilon = \langle \alpha_{\mathcal{S}} \mid \mathcal{S} \in \mathcal{B}^\varepsilon \rangle \text{ and } C^a := \langle \alpha_{\mathcal{T}} \mid \mathcal{T} \in \mathcal{B}^a \rangle$$

In particular, for $\mathcal{S} \in \mathcal{B}^\varepsilon$ and $\mathcal{T} \in \mathcal{B}^a$,

$$\sum_{\theta_a \in \mathcal{S}} a = 0, \tag{5.1}$$

and

$$\sum_{a \in \mathcal{T}} a = 0, \quad \sum_{a \in \mathcal{T}} \theta_0(a) = 0 \tag{5.2}$$

Lemma 5.1. *The respective expression* (5.1), (5.2) *holds for all* $\alpha_{\mathcal{S}} \in C^\varepsilon$, $\alpha_{\mathcal{T}} \in C^a$, *where* $\mathcal{S} \subseteq \Omega^\varepsilon$ *and* $\mathcal{T} \subseteq V$.

Proof. Let $\alpha_{\mathcal{X}}$ and $\alpha_{\mathcal{Y}}$ be two vertices in W^ε with

$$\sum_{\theta_a \in \mathcal{X}} a = \sum_{\theta_a \in \mathcal{Y}} a = 0.$$

As $\mathrm{supp}(\alpha_{\mathcal{X}} + \alpha_{\mathcal{Y}}) = \mathcal{X} \triangle \mathcal{Y}$, the symmetric difference of $\mathcal{X}$ and $\mathcal{Y}$, it follows that

$$\sum_{\theta_a \in \mathcal{X} \triangle \mathcal{Y}} a = \sum_{\theta_a \in \mathcal{X} \triangle \mathcal{Y}} a + \sum_{\theta_a \in \mathcal{X} \cap \mathcal{Y}} 2a = \sum_{\theta_a \in \mathcal{X}} a + \sum_{\theta_a \in \mathcal{Y}} a = 0.$$

Since (5.1) holds for all $\alpha_{\mathcal{S}}$ such that $\mathcal{S} \in \mathcal{B}^\varepsilon$, the assertion now follows. An analogous argument shows that (5.2) holds for all $\alpha_{\mathcal{T}} \in C^a$. □

Corollary 5.2. C^ε *and* C^a *consist entirely of codewords of even weight and both codes have minimum distance* $d = 4$. *Moreover, the sets of codewords of weight* 4 *are in bijection with* $\mathcal{B}^\varepsilon$ *and* $\mathcal{B}^a$ *respectively and*

$$C^\varepsilon = \langle \alpha_{\mathcal{S}} \mid |\mathcal{S}| = 4, \sum_{\theta_a \in \mathcal{S}} a = 0 \rangle, \text{ and } C^a = \langle \alpha_{\mathcal{T}} \mid |\mathcal{T}| = 4, \sum_{a \in \mathcal{T}} a = 0, \sum_{a \in \mathcal{T}} \theta_0(a) = 0 \rangle.$$

Proof. We only treat the code C^a, since a similar argument also holds for C^ε. As C^a is generated by codewords with weight 4, it follows that it consists entirely of codewords with even weight. Suppose there exists $\alpha_\mathcal{T} \in C^\varepsilon$ with weight 2, so $\mathcal{T} = \{v, w\}$ for some $v \neq w$. Then Lemma 5.1 implies that $v + w = 0$, a contradiction, hence $d = 4$. Now let $\alpha_\mathcal{T}$ be any weight 4 vertex in W^a that satisfies (5.2), with $\mathcal{T} = \{v_1, v_2, v_3, v_4\}$. Then (5.2) implies that $v_4 = v_1 + v_2 + v_3$ and $\sum_{i=1}^3 \theta_0(v_i) = \theta_0(\sum_{i=1}^3 v_i)$. In particular, $\mathcal{T} \in \mathcal{B}^a$. Now, by Lemma 5.1, all codewords of weight 4 satisfy (5.2), which proves the second statement. □

5.1. **Covering radius and complete transitivity.** We next give succinct descriptions of the codewords of C^ε and C^a.

Lemma 5.3. *The following hold:*

(a) *For $m \geqslant 4$ and $\alpha_\mathcal{S} \in W^\varepsilon$, $\alpha_\mathcal{S} \in C^\varepsilon$ if and only if $|\mathcal{S}| = 2k$ for some $k \geqslant 2$ and $\sum_{\theta_a \in \mathcal{S}} a = 0$.*

(b) *Let $m \geqslant 3$ and $\alpha_\mathcal{S} \in W^a$. Then $\alpha_\mathcal{S} \in C^a$ if and only if $|\mathcal{S}| = 2k$ for some $k \geqslant 2$, $\sum_{s\in\mathcal{S}} s = 0$ and $\sum_{s\in\mathcal{S}} \theta_0(s) = 0$.*

Proof. In both (a) and (b), the forward implication is a consequence of Lemma 5.1 and Corollary 5.2, and the reverse implication for $k = 2$ also follows from Corollary 5.2. We first prove the reverse implication for (a), that is we prove:

$$|\mathcal{S}| = 2k \text{ for some } k \geqslant 2 \text{ and } \sum_{\theta_a \in \mathcal{S}} a = 0 \Longrightarrow \alpha_\mathcal{S} \in W^\varepsilon. \tag{5.3}$$

Suppose we have verified (5.3) when $k = 3$ and assume (by induction) that (5.3) holds for all $\mathcal{S}$ with $|\mathcal{S}| = 2\ell$ and $\ell < k$. Write $\alpha := \alpha_\mathcal{S}$ for short and assume that $k > 3$. If there exist $\theta_x, \theta_y, \theta_z \in \mathcal{S}$ such that $\theta_0(x + y + z) = \varepsilon$ then $\alpha_{\mathcal{S}'} \in C^\varepsilon$ where $\mathcal{S}' = \{\theta_x, \theta_y, \theta_z, \theta_{x+y+z}\}$. Since $|\operatorname{supp}(\alpha + \alpha_{\mathcal{S}'})| < 2k$, it follows from Lemma 5.1 that $\alpha + \alpha_{\mathcal{S}'}$ statisfies the inductive hypothesis. Thus $\alpha + \alpha'_\mathcal{S} \in C^\varepsilon$, and so $\alpha \in C^\varepsilon$.

We may, therefore, restrict to the case where

$$\theta_0(x + y + z) = 1 - \varepsilon \text{ for all } \theta_x, \theta_y, \theta_z \in \mathcal{S}. \tag{5.4}$$

Now, for any $\theta_x, \theta_y, \theta_z, \theta_s \in \mathcal{S}$, there exist $t, u \in V^\varepsilon$ such that

$$x + y + z + s = t + u \tag{5.5}$$

by Lemma 3.3. Since the four elements of $\mathcal{S}$ distinct, $\{t, u\}$ is not a subset of $\{x, y, z, s\}$. Furthermore, if $\{x, y, z, s\} \cap \{t, u\} \neq \emptyset$, so that $x = t$ say, then (5.5) implies that $y + z + s = u$ and then (5.4) gives

$$1 - \varepsilon = \theta_0(y + z + s) = \theta_0(u) = \varepsilon,$$

a contradiction. We deduce that $\{x, y, z, s\} \cap \{t, u\} = \emptyset$. Now, by induction $\alpha_{\mathcal{S}'} \in C^\varepsilon$ where $\mathcal{S}' = \{\theta_x, \theta_y, \theta_z, \theta_s, \theta_t, \theta_u\}$. Moreover, $|\operatorname{supp}(\alpha+\alpha_{\mathcal{S}'})| < |\mathcal{S}|$ and as before, $\alpha \in C^\varepsilon$.

It thus remains to verify (5.3) in the case where $k = 3$. Since $6 > 4 = 2^2$ at least 3 of the vectors associated with the forms in $\mathcal{S}$ are linearly independent. Since the sum of 6 distinct vectors in $\mathbb{F}_2^3$ cannot be 0, at least 4 of the vectors associated with the forms in $\mathcal{S}$ are linearly independent. Further, an identical argument to that given in the first paragraph shows that we may assume (5.4) holds for $\mathcal{S}$.

Let $\{a_1, a_2, a_3, a_4\}$ be the four linearly independent vectors, so that $\mathcal{S} = \{\theta_{a_1}, \theta_{a_2}, \theta_{a_3}, \theta_{a_4}, \theta_r, \theta_s\}$ for some $\theta_r, \theta_s \in \Omega^\varepsilon$. By the pigeonhole principle there

exist two equal elements in the set $\{\varphi(a_1,a_3),\varphi(a_2,a_3),\varphi(a_4,a_3)\}$, $\varphi(a_1,a_3)$ and $\varphi(a_2,a_3)$ say. By Lemma 3.6 we may choose

$$x \in L(a_1+a_2,\theta_0(a_1+a_2)) \cap L(a_3,\varphi(a_1,a_3)+1) \cap L(a_3+a_4,\theta_0(a_3+a_4)),$$

so that $\theta_0(x)=\varepsilon$. This implies that $x \notin \{a_1,a_2\}$ and since

$$\theta_0(x+a_1+a_2)=\theta_0(x)+\theta_0(a_1+a_2)+\varphi(x,a_1+a_2)=\theta_0(x)=\varepsilon,$$

$\mathcal{S}'=\{\theta_x,\theta_{x+a_1+a_2},\theta_{a_1},\theta_{a_2}\}$ is the support of some codeword $\alpha_{\mathcal{S}'}$. Now, as (5.4) holds, 0 or 1 elements in the set $\{x,x+a_1+a_2\}$ lie in $\{a_3,a_4,r,s\}$. If it is 1 then we must have $\alpha+\alpha_{\mathcal{S}'}\in C^\varepsilon$, so that $\alpha\in C^\varepsilon$. If it is 0 then

$$\operatorname{supp}(\alpha+\alpha_{\mathcal{S}'})=\{\theta_x,\theta_{x+a_1+a_2},\theta_{a_3},\theta_{a_4},\theta_r,\theta_s\},$$

and

$$\begin{aligned}\theta_0((x+a_1+a_2)+r+s)&=\theta_0(x+a_3+a_4)\\ &=\theta_0(x)+\theta_0(a_3+a_4)+\varphi(x,a_3+a_4)=\theta_0(x)=\varepsilon\end{aligned}$$

so that $\alpha+\alpha_{\mathcal{S}'}=\alpha_{\mathcal{T}}+\alpha_{\mathcal{U}}$ where

$$\mathcal{T}:=\{\theta_{x+a_1+a_2},\theta_r,\theta_s,\theta_{x+a_1+a_2+r+s}\} \text{ and } \mathcal{U}:=\{\theta_x,\theta_{a_3},\theta_{a_4},\theta_{x+a_3+a_4}\}.$$

Clearly both $\alpha_{\mathcal{T}}$ and $\alpha_{\mathcal{U}}$ lie in C^ε, so that $\alpha\in C^\varepsilon$ in this case also. This completes the proof of (a).

We next prove the reverse implication for (b). Note first that

$$\sum_{s\in\mathcal{S}}\theta_0(s)=\sum_{s\in\mathcal{S}'}\theta_0(s)=0 \Rightarrow \sum_{s\in\mathcal{S}\triangle\mathcal{S}'}\theta_0(s)=0.$$

The proof is again by induction on k, where we assume that $k\geqslant 3$. Since $\sum_{s\in\mathcal{S}}s=0$, $\langle s \mid s\in\mathcal{S}\rangle$ is a subspace of dimension at least 4 and we may pick be 4 linearly independent vectors in $\mathcal{S}$, a_1,a_2,a_3,a_4 say. By the pigeonhole principle, there exist two elements $s,t\in\{a_1,a_2,a_3,a_4\}$, with $\theta_0(s)=\theta_0(t)$. Without loss of generality, $s=a_1$, $t=a_2$. By [10, Lemma 7.7B], we may choose

$$x\in L(a_1+a_2,\varphi(a_1,a_2))\cap L(a_3+a_4,\varphi(a_3,a_4))$$

with the property that $\theta_0(x)\neq\theta_0(a_1)$. Note in particular that this implies that $x\notin\{a_1,a_2\}$ and

$$\theta_0(x+a_1+a_2)=\theta_0(x)+\theta_0(a_1)+\theta_0(a_2).$$

If $|\mathcal{S}\triangle\{x,a_1,a_2,x+a_1+a_2\}|<2k$, then the lemma holds by induction. Otherwise we have $x\notin\{a_3,a_4\}$ and

$$\theta_0(x+a_3+a_4)=\theta_0(x)+\theta_0(a_3)+\theta_0(a_4),$$

and hence $|(\mathcal{S}\triangle\{x,a_1,a_2,x+a_1+a_2\})\triangle\{x,a_3,a_4,x+a_3+a_4\}|<2k$ and the lemma holds by induction in this case also. The proof is complete.

□

We next show how to identify a certain code constructed in [3] with our code C^a. This will allow us to prove Theorem C (b). We begin by reviewing the construction from [3]. Let $\mathbf{H}$ be the $2m\times(2^{2m}-1)$ parity check matrix of the $[2^{2m}-1,2^{2m}-2m-1,3]$ linear Hamming code, whose columns $c_1,\ldots,c_{2^{2m}-1}$ correspond to the non-zero elements of $(\mathbb{F}_2)^{2m}$. Let $q:V\to\mathbb{F}_2$ be the "bent function" defined by

$$q(v)=\begin{cases}1, & \text{if } wt(v)\equiv 2,3 \mod 4;\\ 0, & \text{otherwise.}\end{cases}$$

In [3] it is shown that q is quadratic, that is, $q(v+w)+q(v)+q(w)$ is a bilinear form on V, and that $q(v) = vQv^T$ where Q is the all ones upper triangular matrix with zeroes on the diagonal.

Let x be the row vector of length $2^{2m}-1$ with $x_i := q(c_i)$ and form a new matrix $\mathbf{H}_x$ from $\mathbf{H}$ by letting x be an additional row. Now let C_x be the code that has $\mathbf{H}_x$ as its parity check matrix, and let C be the *extended code* of C_x, that is, the code obtained from C_x via the addition of an extra coordinate so that the sum of the coordinates of the extended codeword is zero. Thus codewords in C may be identified with vectors $\alpha_{\mathcal{S}}$ ($\mathcal{S} \subseteq V$) with the property that

$$|\mathcal{S}| \text{ is even, } \sum_{v\in\mathcal{S}} v = 0 \text{ and } \sum_{v\in\mathcal{S}} q(v) = 0.$$

Writing $\psi(v_1, v_2) := q(v_1+v_2)+q(v_1)+q(v_2)$, we note that ψ is a non-degenerate symplectic bilinear form on V. This means that there exists a matrix $A \in \mathrm{GL}(V)$ with

$$\psi(uA, vA) = \varphi(u, v)$$

for each $u, v \in V$ where φ is the form of Section 3 to which θ_0 polarises [24].

Now define a map

$$\rho_A : C^a \to C, \;\; \alpha_{\mathcal{T}} \mapsto \alpha_{\mathcal{S}}$$

where $\mathcal{T} \subseteq V$ and $\mathcal{S} := \{tA \mid t \in \mathcal{T}\}$. We claim that ρ_A is an isomorphism of codes.

We show first that the image of ρ_A is a subset of C. Suppose that $\alpha_{\mathcal{T}} \in C^a$, so

$$|\mathcal{T}| \text{ is even, } \sum_{v\in\mathcal{T}} v = 0 \text{ and } \sum_{v\in\mathcal{T}} \theta_0(v) = 0. \tag{5.6}$$

Clearly $|\mathcal{S}|$ is even and

$$\sum_{u\in\mathcal{S}} u = \sum_{v\in\mathcal{T}} vA = \left(\sum_{v\in\mathcal{T}} v\right) A = 0.$$

It thus remains to show that

$$\sum_{u\in\mathcal{S}} q(u) = 0.$$

We define

$$q_A : V \to \mathbb{F}_2, \;\; v \mapsto q(vA)$$

and observe that

$$\sum_{u\in\mathcal{S}} q(u) = \sum_{v\in\mathcal{T}} q(vA) = \sum_{v\in\mathcal{T}} q_A(v).$$

Furthermore, for each $u, v \in V$,

$$\begin{aligned} q_A(v_1) + q_A(v_2) + qA(v_1+v_2) &= q(v_1A) + q(v_2A) + q((v_1+v_2)A) \\ &= q(v_1A) + q(v_2A) + q(v_1A + v_2A) \\ &= \psi(v_1A, v_2A) \\ &= \varphi(v_1, v_2). \end{aligned}$$

We conclude that q_A is a form on V which polarises to φ. Hence $q_A = \theta_a$ for some $a \in V$ (by results in [10, Section 7.7], as discussed at the start of Section 3). But

now,

$$\begin{array}{ll} \sum_{v\in\mathcal{T}} q_A(v) & = \sum_{v\in\mathcal{T}} \theta_a(v) \\ & = \sum_{v\in\mathcal{T}} \theta_0(v) + \sum_{v\in\mathcal{T}} \varphi(a,v) \quad \text{(definition of } \theta_a\text{)} \\ & = 0 + \varphi(a, \sum_{v\in\mathcal{T}} v) \quad \text{(by (5.6))} \\ & = \varphi(a,0) \quad \text{(by (5.6))} \\ & = 0, \end{array}$$

as required. We know, then, that $\rho_A : C^a \to C$ is a well-defined map; now the fact that it is a bijection follows directly from the fact that it has an obvious inverse.

Theorem 5.4. *$C_{\mathbb{F}_2}(\mathcal{D}^a)$ is a completely transitive $[2^{2m}, 2^{2m}-(2m+2), 4]$ code with covering radius 4 and intersection array*

$$(2^{2m}, 2^{2m}-1, 2^{2m-1}, 1; 1, 2^{2m-1}, 2^{2m}-1, 2^{2m}).$$

Proof. This follows from [3, Theorem 2.4]. □

We are left with the task of proving Theorem C (a). Recall from Section 2 the notation

$$C_i^\varepsilon := \{\beta \in W^\varepsilon \mid \min_{\alpha\in C^\varepsilon} d(\beta,\alpha) = i\}.$$

Our next result shows that $C_i^\varepsilon = \emptyset$ for all $i \geqslant 4$ (so C_i^ε has covering radius 3) from which we can quickly deduce that C^ε is a completely transitive code.

Proposition 5.5. *Let $m \geqslant 4$ and $\varepsilon \in \mathbb{F}_2$. For each $\alpha_\mathcal{S} \in W^\varepsilon$ with $\mathcal{S} := \mathrm{supp}(\alpha_\mathcal{S})$ and $v := \sum_{a\in\mathcal{S}} a$, one of the following holds:*

(i) *$|\mathcal{S}|$ is even, $v = 0$ and $\alpha_\mathcal{S} \in C_0^\varepsilon$;*
(ii) *$|\mathcal{S}|$ is odd, $v \in V^\varepsilon$ and $\alpha_\mathcal{S} \in C_1^\varepsilon$;*
(iii) *$|\mathcal{S}|$ is even, $v \neq 0$ and $\alpha_\mathcal{S} \in C_2^\varepsilon$;*
(iv) *$|\mathcal{S}|$ is odd, $v \in V^{1-\varepsilon}$ and $\alpha_\mathcal{S} \in C_3^\varepsilon$.*

Consequently, C^ε has covering radius 3.

Proof. Suppose that $|\mathcal{S}|$ is even. If $v = 0$, then by Lemma 5.3 $\alpha_\mathcal{S} \in C^\varepsilon$ and (i) holds, so we may assume that $v \neq 0$. By Lemma 3.3, $v = x+y$ for distinct elements $x, y \in V^\varepsilon$. Set $\alpha' := \alpha_\mathcal{S} + \alpha_{\mathcal{S}'}$, where $\mathcal{S}' = \{\theta_x, \theta_y\}$, so that

$$\mathrm{supp}(\alpha') = \mathcal{S}\Delta\mathcal{S}' \text{ and } \sum_{\theta_a\in\mathrm{supp}(\alpha')} a = 0.$$

In particular, $\alpha' \in C^\varepsilon$ and $d(\alpha_\mathcal{S}, \alpha') = 2$. Now (iii) follows because C^ε has minimum distance $d = 4$.

Next suppose that $|\mathcal{S}|$ is odd. If $v \in V^\varepsilon$ then $\alpha' = \alpha_\mathcal{S} + \alpha_{\{\theta_v\}}$ is a codeword with $d(\alpha_\mathcal{S}, \alpha') = 1$ so that (ii) holds. If $v \in V^{1-\varepsilon}$ then by Corollary 3.4, there exist $x, y, z \in V^\varepsilon$ such that $v = x+y+z$. In this case $\alpha' = \alpha_\mathcal{S} + \alpha_{\{\theta_x,\theta_y,\theta_z\}}$ is a codeword with $d(\alpha_\mathcal{S}, \alpha') = 3$ and (iv) holds.

□

Corollary 5.6. *For each $m \geqslant 3$ and $\varepsilon \in \mathbb{F}_2$, C^ε is a completely transitive code with covering radius 3.*

Proof. By Proposition 5.5, C^ε has covering radius 3 for $m \geqslant 4$, and using GAP [11], we verify this to hold when $m = 3$ also. Thus we need to show that $\mathrm{Aut}(C^\varepsilon)$ is transitive on C_i^ε for $i = 0, 1, 2, 3$. Since C^ε is generated by the rows of the incidence matrix of $\mathcal{D}^\varepsilon$, and because $\mathcal{D}^\varepsilon$ is a $\mathrm{Sp}_{2m}(2)$-orbit, it follows that $\mathrm{Aut}(C^\varepsilon) \geqslant N_{C^\varepsilon} \rtimes$

$\mathrm{Sp}_{2m}(2)$, where N_{C^ε} is the group of translations of C^ε. As N_{C^ε} acts regularly on C^ε, $\mathrm{Sp}_{2m}(2)$ acts 2-transitively on entries and C^ε has minimum distance $d = 4$, we deduce that C^ε, C_1^ε and C_2^ε are all $\mathrm{Aut}(C^\varepsilon)$-orbits. Let $\nu_1, \nu_2 \in C_3^\varepsilon$. As $\mathrm{Aut}(C^\varepsilon)$ acts transitively on C^ε, we can assume that $\nu_1, \nu_2 \in \Gamma_3(0) \cap C_3^\varepsilon$. (Recall that $\Gamma_i(\alpha) = \{\beta \in W^\varepsilon \mid d(\beta, \alpha) = i\}$.) It is straightforward to show that both $\Gamma_3(0) \cap C_1$ and $\Gamma_3(0) \cap C_3$ are non-empty sets. Thus $\mathrm{Sp}_{2m}(2)$ has at least 2 orbits on $\Gamma_3(0)$. But, by Theorem 3.5, $\mathrm{Sp}_{2m}(2)$ has exactly two orbits on $\Gamma_3(0)$. Hence there exists $g \in \mathrm{Sp}_{2m}(2)$ such that $\nu_1^g = \nu_2$, proving that C_3^ε is an $\mathrm{Aut}(C^\varepsilon)$-orbit, and therefore, C^ε is completely transitive. □

5.2. **Dimension of C^ε and completing the proof of Theorem C.** By Proposition 5.5, we must have

$$2^{n^\varepsilon} = |W^\varepsilon| = |C^\varepsilon| \sum_{i=0}^{3} \mu_i. \tag{5.7}$$

where $n^\varepsilon = |\Omega^\varepsilon|$ and μ_i denotes the number of cosets of C^ε of weight i. Thus, in the next result, we calculate μ_i for $i = 0, 1, 2, 3$ which allows us to determine the dimension of C^ε.

Proposition 5.7. *For each $m \geqslant 3$ and $\varepsilon \in \mathbb{F}_2$, let $f_\varepsilon(m) := 2^{m-1} \cdot (2^m + (-1)^\varepsilon)$. Then C^ε is a $[f_\varepsilon(m), f_\varepsilon(m) - (2m+1), 4]$ completely transitive code with intersection array*

$$(f_\varepsilon(m), f_\varepsilon(m) - 1, f_\varepsilon(m) - 2f_\varepsilon(m-1); 1, 2f_\varepsilon(m-1), f_\varepsilon(m)).$$

Proof. Write $n^\varepsilon := f_\varepsilon(m)$ for short. By Proposition 5.5 and Corollary 5.6, C^ε is completely transitive (and therefore completely regular) with covering radius 3. Let $(b_0, b_1, b_2; c_1, c_2, c_3)$ be the intersection array of C^ε. As C^ε has minimum distance $d = 4$, it follows that $b_0 = n^\varepsilon$, $b_1 = n^\varepsilon - 1$ and $c_1 = 1$. As C^ε is generated by codewords of weight 4, it consists entirely of codewords of even weight. From this we deduce that for any $\nu \in C_i$, there are no neighbours of ν in C_i, that is, $n^\varepsilon - b_i - c_i = 0$ (so $b_i + c_i = n^\varepsilon$) for $i = 0, 1, 2, 3$. Therefore $c_3 = n^\varepsilon$. Now let $\nu \in C_2^\varepsilon$, and without loss of generality, assume that ν has weight 2. Clearly ν has exactly two neighbours of weight 1 in C_1^ε, so the number $c_2 - 2$ is equal to the number of weight 3 neighbours of ν that are also covered by a codeword of weight 4. By Corollary 5.2, the codewords of weight 4 form a $2-(n^\varepsilon, 4, \lambda^\varepsilon)$ design where $\lambda^\varepsilon = 2^{m-2}(2^{m-1} + (-1)^\varepsilon) - 1 = f_\varepsilon(m-1) - 1$, so there exist λ^ε codewords of weight 4 that cover ν. Each contributes 2 neighbours of ν of weight 3 that are in C_1^ε. Hence $c_2 = 2\lambda^\varepsilon + 2$, and thus $b_2 = n^\varepsilon - 2\lambda^\varepsilon - 2$. Applying Lemma 2.3 to the intersection array gives

$$\mu_0 = 1,\ \mu_1 = n^\varepsilon,\ \mu_2 = \frac{n^\varepsilon(n^\varepsilon - 1)}{2\lambda^\varepsilon + 2},\ \mu_3 = \frac{(n^\varepsilon - 1)(n^\varepsilon - 2\lambda^\varepsilon - 2)}{2\lambda^\varepsilon + 2}.$$

Thus

$$2^{n^\varepsilon} = |W^\varepsilon| = |C^\varepsilon|(1 + n^\varepsilon + \frac{n^\varepsilon(n^\varepsilon - 1)}{2\lambda^\varepsilon + 2} + \frac{(n^\varepsilon - 1)(n^\varepsilon - 2\lambda^\varepsilon - 2)}{2\lambda^\varepsilon + 2}).$$

But

$$n^\varepsilon + \frac{(n^\varepsilon - 1)(n^\varepsilon - 2\lambda^\varepsilon - 2)}{2\lambda^\varepsilon + 2} = \frac{n^\varepsilon(n^\varepsilon - 1)}{2\lambda^\varepsilon + 2} + 1 = 2^{2m},$$

which implies that the dimension of C^ε is $n^\varepsilon - (2m + 1)$. □

Proof of Theorem C. This follows immediately from Theorem 5.4 and Propositions 5.5 and 5.7. □

6. Conway groupoids with large support

In this section we prove Theorem D. Although Theorem D is stated in terms of $\mathcal{L}_\infty(\mathcal{D})$, it will be convenient to work instead with the hole stabilizer $G = \pi_\infty(\mathcal{D})$. This approach is advantageous because of the extra flexibility afforded to us from knowing that G is a group.

In light of this we record the following statement which is equivalent to Theorem D.

Theorem 6.1. *Suppose that $\mathcal{D}$ is a supersimple $2-(n,4,\lambda)$ design and that $G := \pi_\infty(\mathcal{D})$ is the associated hole-stabilizer. Suppose, furthermore, that $[\infty, a, b, \infty] = 1$ whenever ∞ is collinear with $\{a, b\}$. Then one of the following is true:*

1. *$\mathcal{D}$ is a Boolean design and G is trivial;*
2. *$\mathcal{D} = \mathbb{P}_3$ (the projective plane of order 3) and $G \cong M_{12}$; or*
3. *$G = \mathrm{Alt}(n-1)$.*

The fact that Theorem 6.1 is equivalent to Theorem D can be proved using [12, Theorem B], [8, Proposition 3.4], and [12, Lemma 3.1]. Throughout this section we operate under the suppositions of Theorem 6.1.

6.1. Background results.

We start by collecting a number of important background results.

For a permutation group H acting on a set of size d we write $\mu(H)$ for the smallest number of elements moved by a non-trivial element of H (i.e. $\mu(H)$ is the size of the smallest possible support of a non-trivial element of H). In what follows we will use the crucial fact that if H is primitive and doesn't contain $\mathrm{Alt}(d)$, then $\mu(H)$ is bounded below by a function of d.

The following theorem is due to Liebeck and Saxl [15], and makes use of the Classification of Finite Simple Groups.

Theorem 6.2. *Let d be a positive integer and let H be a primitive subgroup of $\mathrm{Sym}(d)$ that does not contain $\mathrm{Alt}(d)$. Either $\mu(H) \geqslant \frac{1}{3}d$ or $(\mathrm{Alt}(m))^r \trianglelefteq G \leqslant \mathrm{Sym}(m) \wr \mathrm{Sym}(r)$ where $m \geqslant 5$ and the wreath product acts, via the product action on $\Omega = \Delta^r$ and Δ is either the set of ℓ-subsets of $\{1, \dots, m\}$ ($1 \leqslant \ell < \frac{1}{2}m$) or $m = |\Delta| = 6$. In particular, in all cases, $\mu(H) \geqslant 2(\sqrt{d} - 1)$.*

Observe that Theorem 6.2 implies that either $\mu(H) \geqslant \frac{1}{3}d$ or else we have that $d = \binom{m}{\ell}^r$ or 6^r.

We will also need an elementary result from number theory, which can be regarded as a special case of Mihăilescu's theorem, formerly the Catalan conjecture [19].

Lemma 6.3. *Suppose that a, b, p are positive integers, that $a, b > 1$ and that $p^a \pm 1 = 2^b$. Then either $a = 1$ or $p = 3, a = 2$.*

Proof. If a is odd then the second factor in $p^a \pm 1 = (p \pm 1)(p^{a-1} \mp \ldots + 1)$ is odd. Hence $a - 1 = 0$ in this case. If $a = 2t$ for some $t > 0$ then there are two possibilities: firstly, we could have $2^b = (p^{2t} - 1) = (p^t - 1)(p^t + 1)$ and we obtain immediately that $(p, t, a) = (3, 1, 2)$. Secondly, we could have $2^b = p^{2t} + 1$; but since $p^{2t} + 1 \equiv 2 \mod 4$, this yields no solutions. □

6.2. **A structure result.** Our main tool for proving Theorem D will be the following proposition that provides a detailed description of the structure of a design satisfying the suppositions of Theorem D.

Proposition 6.4. *Suppose that $\mathcal{D}$ is a supersimple $2-(n,4,\lambda)$ design, and that G contains no non-trivial elements of the form $g=[\infty,a,b,\infty]$ where $\infty\in\overline{a,b}$. Then $\lambda=2^\alpha-1$ for some positive integer α, and any two points a and b lie in a unique Boolean $3-(2^{\alpha+1},4,1)$ subdesign $\mathcal{D}_{a,b}$. Moreover, writing $\Lambda:=\{\overline{a,b}\mid a,b\in\Omega, a\neq b\}$, the pair (Ω,Λ) is a $2-(n,2^{\alpha+1},1)$ design.*

For a definition of the Boolean $3-(2^k,4,1)$ design we refer the reader to [12, Section 2]. Notice that when $\alpha=1$, Proposition 6.4 is true but gives no information: in this case we have $\lambda=1$, the Boolean subdesign $\mathcal{D}_{a,b}$ is the trivial design containing 1 line and the pair (Ω,Λ) is just the original design $\mathcal{D}$.

Notice too that a sort of converse of Proposition 6.4 is true: one can start with a $2-(n,2^{\alpha+1},1)$ design, "replace" each of its lines with a Boolean $3-(2^{\alpha+1},4,1)$ subdesign and one will thereby obtain a $2-(n,4,2^\alpha-1)$ design for which the move sequence $[\infty,a,b,\infty]$ is trivial whenever $\infty\in\overline{a,b}$.

Lemma 6.5. *Let $(\Omega,\mathcal{B})$ be a supersimple $2-(n,4,\lambda)$ design, and let a,b,c be distinct points in Ω such that $c\in\overline{a,b}$ and $[c,a,b,c]=1$. Then $\overline{a,c}=\overline{a,b}=\overline{b,c}$.*

Proof. Let $g=[c,a,b,c]$ and $x\in\overline{a,c}$, so $\{a,c,x,y\}$ is a line for some $y\in\Omega\backslash\{a,c,x\}$. If $x\notin\overline{a,b}\cup\overline{b,c}$, then $y^g=x$, which is a contradiction. If $x\notin\overline{a,b}\cap\overline{b,c}$, then one of $\{a,b,x,y\}$ or $\{b,c,x,y\}$ is a line, contradicting supersimplicity. Thus, as $|\overline{a,c}|=|\overline{a,b}|=|\overline{b,c}|=2\lambda+2$, the result holds. □

Let $\mathcal{D}=(\Omega,\mathcal{B})$ be a $2-(n,4,\lambda)$ design. Then, for $r,s\in\Omega$, with $r\neq s$, let $\mathcal{B}(r,s)$ denote the set of λ lines in $\mathcal{B}$ that contain both r and s.

Lemma 6.6. *Let $(\Omega,\mathcal{B})$ be a supersimple $2-(n,4,\lambda)$ design with the property that for all distinct pairs $a,b\in\Omega$ and for all $c\in\overline{a,b}$, $[c,a,b,c]=1$. Then $\mathcal{D}_{a,b}=(\Omega_{a,b},\mathcal{B}_{a,b})$ is a $3-(2\lambda+2,4,1)$ design, where $\Omega_{a,b}=\overline{a,b}$ and*

$$\mathcal{B}_{a,b}=\bigcup_{\substack{r,s\in\overline{a,b}\\ r\neq s}}\mathcal{B}(r,s).$$

Moreover, $\mathcal{D}_{a,b}$ is a Boolean quadruple system of order $2^{\alpha+1}$ for some $\alpha>0$. Consequently, $\lambda=2^\alpha-1$.

Proof. Let y,r,s be three distinct points in $\overline{a,b}$. We show that y,r,s lie in a unique element of $\mathcal{B}_{a,b}$. Suppose first that both a and b lie in the set $\{y,r,s\}$, with $r=a$ and $s=b$ say. As $y\in\overline{a,b}$, there exists a line $\ell\in\mathcal{B}$ (which is necessarily in $\mathcal{B}(a,b)$) that contains all three points, and by supersimplicity, this line is unique. Secondly, suppose that at most one of a,b lies in $\{y,r,s\}$, so we may assume that $a,b\notin\{r,s\}$. Then $[r,a,b,r]=[s,a,b,s]=1$, and by Lemma 6.5, $\overline{a,r}=\overline{a,b}=\overline{a,s}$, so $s\in\overline{a,r}$. Now, by supposition, $[s,a,r,s]=1$, from which we deduce that $\overline{r,s}=\overline{a,b}$. Thus $y\in\overline{a,b}\backslash\{r,s\}=\overline{r,s}\backslash\{r,s\}$, and so y,r,s are contained in a line in $\mathcal{B}$ (which is in $\mathcal{B}(r,s)$) and by supersimplicity, this line is unique. Therefore $\mathcal{D}_{a,b}$ forms a $3-(2\lambda+2,4,1)$ design, and hence, a supersimple $2-(2\lambda+2,4,\lambda)$ design.

As $y\in\overline{r,s}$, $[y,r,s,y]=1$ by supposition, and because y,r,s were arbitrary, we conclude that $\pi_x(\mathcal{D}_{a,b})=1$ for each $x\in\overline{a,b}$. Hence, $\mathcal{D}_{a,b}$ is a Boolean quadruple system of order 2^α for some $\alpha>0$ by [12, Theorem B]. □

Proof of Proposition 6.4. The first statement of the proposition is a consequence of Lemma 6.6. Thus it remains to show that the pair (Ω, Λ) is a $2-(n, 2^{\alpha+1}, 1)$ design. But each pair of elements $a, b \in \Omega$ is contained in $\overline{a,b}$ and if there exist another pair $x, y \in \Omega$ such that $a, b \in \overline{x,y}$ then $\overline{x,y} = \overline{a,b}$, as is shown in the proof of Lemma 6.6. Consequently $\overline{a,b}$ is the unique element of Λ that contains $\{a, b\}$. □

We record a corollary to Proposition 6.4:

Corollary 6.7. *Suppose that $\mathcal{D}$ is a supersimple $2-(n, 4, \lambda)$ design, and that G contains no non-trivial elements of the form $g = [\infty, a, b, \infty]$ where $\infty \in \overline{a,b}$. If G contains* $\mathrm{Alt}(n-1)$ *then* $G = \mathrm{Alt}(n-1)$

Proof. Proposition 6.4 implies that $\lambda = 2^\alpha - 1$ for some positive integer α and, in particular, λ is odd. Therefore G is generated by even permutations and since $\mathrm{Alt}(n-1) \leqslant G \leqslant \mathrm{Sym}(n-1)$, the result follows. □

6.3. **Proving Theorem D.** Our job now is to prove Theorem D, and to do this we will make heavy use of Proposition 6.4. We will also need to make use of Theorem E part (2), a short proof of which is given in Section 7.1. Note that although the proof of part (4) of Theorem E makes use of Theorem D, the earlier parts do not.

We start with an elementary result from [12] concerning the hole stabilizer $G = \pi_\infty(\mathcal{D})$.

Lemma 6.8. $G = \langle [\infty, a, b, \infty] \mid a, b \in \Omega \backslash \infty \rangle$. *Furthermore the elements $[\infty, a, b, \infty]$ have support of size at most $6\lambda + 2$.*

Proof. See [12, Lemmas 3.1 and 7.3]. □

Next we need an easy corollary to Proposition 6.4.

Corollary 6.9. *Suppose that a hole stabilizer $G = \pi_\infty(\mathcal{D})$ contains no non-trivial elements of the form $g = [\infty, a, b, \infty]$ where $\infty \in \overline{a,b}$. Suppose, furthermore, that G does not equal* $\mathrm{Alt}(n-1)$. *Then $\lambda = 2^\alpha - 1$ for some integer α and (setting $k = 2^{\alpha+1}$), $n = k, k^2-k+1, 2(k^2-k)+1, k^2$ or $2k^2-k$. If $n = k$ then G is trivial; otherwise G is primitive.*

Proof. We apply Proposition 6.4 to deduce the existence of a $2-(n, k, 1)$ design (Ω, Λ). Suppose that the design is trivial, i.e. $n = k$. Then Proposition 6.4 implies that $\mathcal{D}$ is the Boolean design and [12, Theorem B] implies that G is trivial.

Suppose next that the associated $2-(n, k, 1)$ design is non-trivial, i.e. $n > k$. Observe that $k = 2\lambda + 2$ and now Fisher's inequality implies that

$$n > k^2 - k > 9\lambda + 1.$$

Thus, by Theorem E (2), G is primitive.

We know that G is generated by elements of the form $[\infty, a, b, \infty]$ and these have support at most $6\lambda + 2$ by Lemma 6.8. Combining this fact with the inequality $\mu(H) \geqslant 2(\sqrt{d} - 1)$ of Theorem 6.2 (and setting $d = n - 1$) we obtain

$$n \leqslant 9\lambda^2 + 12\lambda + 5 < 3k(k-1).$$

From the fact that (Ω, Λ) is a $2-(n, k, 1)$ design (Proposition 6.4) we also have the divisibility conditions that $k-1$ divides $n-1$ and $k(k-1)$ divides $n(n-1)$ (since the number of lines in a $2-(n, k, 1)$ design is $\frac{n(n-1)}{k(k-1)}$). Note that k is a power of 2.

If n is odd, then $k(k-1)$ divides $n-1$ and we conclude that either $n = k^2-k+1$ or $2(k^2-k)+1$. If n is even, then $k-1$ divides $n-1$ and k divides n. Hence $n-1 = (1+ak)(k-1)$ for some $a > 0$ and we obtain that $n = k^2$ or $2k^2-k$ as required. □

Lemma 6.10. *Suppose that a hole stabilizer $G = \pi_\infty(\mathcal{D})$ contains no non-trivial elements of the form $g = [\infty, a, b, \infty]$ where $\infty \in \overline{a,b}$. Suppose, furthermore, that G is neither trivial nor does it equal $\mathrm{Alt}(n-1)$, and that $\lambda > 1$.Then the following hold:*

(1) *G is primitive.*
(2) *$\lambda = 2^\alpha - 1$ for some integer $\alpha \geqslant 2$ and (setting $k = 2^{\alpha+1}$),*
$$n = k^2-k+1, 2(k^2-k)+1, k^2 \text{ or } 2k^2-k.$$
(3) *There exist integers m, ℓ, r ($m \geqslant 5$, $1 \leqslant \ell < \frac{1}{2}m$) such that $n-1 = \binom{m}{\ell}^r$ or 6^r. Furthermore $(\mathrm{Alt}(m))^r \trianglelefteq G \leqslant \mathrm{Sym}(m) \wr \mathrm{Sym}(r)$ where $m \geqslant 5$ and the wreath product acts, via the product action on $\Omega = \Delta^r$ and Δ is either the set of ℓ-subsets of $\{1, \ldots, m\}$ or $m = |\Delta| = 6$.*

Proof. We apply Corollary 6.9 and observe that, since G is not trivial, $n \neq k$. Thus G is primitive and (1) and (2) hold.

Now observe that $k = 2\lambda + 2$ and that G contains non-trivial elements with support of size at most $6\lambda + 2 = 3k - 4$. If $\lambda \neq 3$, then all four possible values for n are strictly greater than $9k - 11$, hence Theorem 6.2 yields (3).

If $\lambda = 3$, then three of the possible values for n are strictly greater than $9k-11 = 61$ and Theorem 6.2 yields (3). To rule out the final case (when $n = k^2-k+1 = 57$) we use GAP [11] to confirm that none of the primitive groups of degree 56 contain non-trivial elements with support of size at most $6\lambda + 2 = 20$, thus this situation can be excluded entirely. □

Lemma 6.11. *Let $k = 2^{\alpha+1}$ for some integer $\alpha \geqslant 2$, and suppose that $d = k^2 - k$ or $2(k^2-k)$. Then $d \neq 6^r$ and if $d = \binom{m}{\ell}^r$ for positive integers m, ℓ and r with $\ell \leqslant \frac{m}{2}$, then either $(m, \ell, r) = (d, 1, 1)$ or else $(d, k) = (57, 8)$.*

Proof. Suppose that $d = s^r$ for some integer s and observe that d is a product of $k-1$ (an odd number) and a power of 2. Thus $k-1 = s_1^r$ for some integer s_1. Now Lemma 6.3 implies that $r = 1$. One concludes immediately that $d \neq 6^r$.

Suppose that $d = \binom{m}{\ell}$ and $d = k^2 - k$. Observe that d is divisible by $2^{\alpha+1}$. It is trivial to observe that if $2^{\alpha+1}$ divides $\binom{m}{\ell}$, then $m \geqslant 2^{\alpha+1}$ and hence
$$k(k-1) = \binom{m}{\ell} \geqslant \binom{k}{\ell} = \frac{k(k-1)\cdots(k-\ell+1)}{\ell!}.$$
This inequality implies that either $\ell \leqslant 2$ or $k \leqslant 8$. The same conclusion is reached if we assume that $d = \binom{m}{\ell}$ and $d = 2(k^2-k)$: one simply replaces $2^{\alpha+1}$ with $2^{\alpha+2}$ in the given argument.

Suppose that $\ell \leqslant 2$. If $\ell = 2$ then $m(m-1) = 2^x(2^y-1)$, for some integers x, y with $x > y$ which is absurd. Hence $\ell = 1$ and the result follows.

Finally, suppose that $k \leqslant 8$ and $\ell > 2$. Then one obtains immediately that $k = m = 8$, $\ell = 3$, $d = 57$ and the result follows. □

Lemma 6.12. *Let $k = 2^{\alpha+1}$ for some integer $\alpha \geqslant 2$, and suppose that $d = k^2 - 1$ or $2k^2 - k - 1$. Then $d \neq 6^r$ and if $d = \binom{m}{\ell}^r$ for positive integers m, ℓ and r, then $r = 1$.*

Proof. Observe that d is odd, and thus $d \neq 6^r$. Suppose first that

$$d = k^2 - 1 = (k-1)(k+1) = s^r$$

for some positive integers r and s. Then, since $k-1$ and $k+1$ are coprime, we conclude that $k - 1 = s_1^r$ for some positive integer s_1. Now Lemma 6.3 implies that $r = 1$ as required.

Assume, then that $d = 2k^2 - k - 1 = s^r$ for some integer r. There are two cases. First, suppose that $2k+1$ and $k-1$ are coprime. Then $k - 1 = s_1^r$ for some integer s_1 and Lemma 6.3 implies that $r = 1$.

Second, suppose that $2k + 1$ and $k - 1$ are not coprime; then their highest common factor is 3 and we conclude, moreover that $\alpha + 1$ is even. In this case $k - 1 = (\sqrt{k} - 1)(\sqrt{k} + 1)$ and one of these two factors is indivisible by 3.

Suppose first that $\sqrt{k} - 1$ is indivisible by 3. Then $\sqrt{k} - 1$ is coprime to $2k + 1$ and $\sqrt{k} + 1$ and we conclude that $\sqrt{k} - 1 = x^r$ for some integer x. Now Lemma 6.3 implies that $r = 1$ as required.

Suppose finally that $\sqrt{k} + 1$ is indivisible by 3. Then $\sqrt{k} + 1$ is coprime to $2k + 1$ and $\sqrt{k} - 1$ and we conclude that $\sqrt{k} + 1 = x^r$ for some integer x. Now Lemma 6.3 and the fact that $\sqrt{k} + 1$ is indivisible by 3 implies that $r = 1$ as required. □

Lemma 6.13. *Suppose that G is isomorphic to a subgroup of $\mathrm{Sym}(m)$ and consider the natural action of G on the set of ℓ-subsets of $\{1, \ldots, m\}$. Then a non-trivial element of G has support at least $2\binom{m-2}{\ell-1}$.*

Proof. Let g be a non-trivial element of G and let i be an element that is moved by G. Thus $i^g = j$ with $j \neq i$. Let $k = j^g$ and observe that, although it is possible to have $i = k$, we know that $j \neq k$.

Now observe that any set containing i but not j lies in the support of g, and there are $\binom{m-2}{\ell-1}$ of these. Similarly any set containing j but not k lies in the support of g, and there are $\binom{m-2}{\ell-1}$ of these. The two types of set are distinct hence the result follows. □

We remark that if $g \in G$ is a transposition, then the support of g in the given action is of size exactly $2\binom{m-2}{\ell-1}$. We are ready to prove Theorem D.

Proof of Theorem D. If $\lambda = 1$, then the result is a consequence of [12, Theorem C]. If G is trivial, then the result is a consequence of [12, Theorem B]. Thus we assume that $\lambda > 1$ and that G is not trivial and we must show that $G = \mathrm{Alt}(n-1)$.

Suppose, for a contradiction, that G does not equal $\mathrm{Alt}(n-1)$. Then Lemma 6.10 implies that G is primitive and, for each value of λ, gives four possible values for n. For two of these values Lemma 6.11 implies immediately that either G is $\mathrm{Alt}(n-1)$ (and we are done), or else $(n, k) = (57, 8)$. Now GAP [11] confirms that none of the primitive groups of degree 56 contain non-trivial elements with support of size at most $6\lambda + 2 = 20$, thus this situation is excluded.

We are left with the possibility that $n = k^2$ or $2k^2 - k$ where $k = 2\lambda + 2 \geqslant 8$. Now Lemma 6.12 implies that $\mathrm{Alt}(m) \leqslant G \leqslant \mathrm{Sym}(m)$ for some $m \geqslant 5$ and that the action of G on $n - 1$ points is isomorphic to the natural action of G on the set

of ℓ-subsets of $\{1,\dots,m\}$. We know that G contains elements with support of size at most $s = 6\lambda + 2 = 3k - 4$ and we observe that

$$n - 1 \geqslant k^2 - 1 \geqslant \frac{1}{9}s^2.$$

Now Lemma 6.13 implies that m and ℓ satisfy

$$\binom{m}{\ell} \geqslant \frac{4}{9}\binom{m-2}{\ell-1}^2.$$

This implies in turn that

$$m \geqslant \frac{4}{9}\binom{m-2}{\ell-1}$$

and one concludes immediately that either $m \leqslant 8$ or $\ell - 1 = 1$.

Suppose first that $m \leqslant 8$. Then $n - 1 = \binom{m}{\ell} \leqslant 70$ and we conclude that $k = 8$ and $n = k^2$. But there does not exist ℓ such that $n - 1 = 63 = \binom{m}{\ell}$ for any $m \leqslant 8$ so this case can be excluded.

Thus we conclude that $\ell = 2$ and $n \in \{k^2, 2k^2 - k\}$. If $n = 2k^2 - k$ then

$$n - 1 = (2k + 1)(k - 1) = \frac{1}{2}m(m - 1)$$

and so

$$(2k + 1)(2k - 2) = m(m - 1).$$

Clearly $2k - 1 < m < 2k + 1$ but, on the other hand, $m = 2k$ does not yield an inequality. Thus we have a contradiction. If $n = k^2$, then

$$n - 1 = (k - 1)(k + 1) = \frac{1}{2}m(m - 1).$$

In this case the action of G on $\Omega\backslash\{\infty\}$ is isomorphic to the action of G on the set of all 2-subsets of $\{1,\dots,m\}$. Let $g \in G$ be the product of t distinct transpositions in $\mathrm{Sym}(m)$. A straighforward calculation yields that

$$|\operatorname{supp}(g)| = -2t^2 + (2m - 2)t.$$

Next observe that, if $a, b \in \Omega \setminus \{\infty\}$ such that $\infty \notin \overline{a, b}$, then $h = [\infty, a, b, \infty]$ is an involution of support exactly $6\lambda + 2$. (This is a consequence of the fact that, since $\mathcal{D}$ is constructed from a $2 - (n, k, 1)$ design, the pairwise intersections of the three sets $\overline{\infty, a}$, $\overline{\infty, b}$ and $\overline{a, b}$ are all subsets of $\{a, b, \infty\}$.)

Now we use the fact that $n = k^2$, $k = 2^{\alpha+1}$ and $\lambda = 2^\alpha - 1$. Then observe that

$$\frac{m(m-1)}{2} = n - 1 = 2^{2\alpha+2} - 1$$

and so $m < 2^{\alpha+2}$. On the other hand, the observations of the previous paragraph imply that

$$-2t^2 + (2m - 2)t = 6\lambda + 2 = 6 \cdot 2^\alpha - 4$$

for some $t \in \{1,\dots,\lfloor \frac{m}{2} \rfloor\}$. Rearranging we obtain that

$$m = \frac{3 \cdot 2^\alpha - 2}{t} + t + 1.$$

Write $g(t) = \frac{3\cdot 2^\alpha - 2}{t} + t + 1$. Now, since $t \leqslant \lfloor \frac{m}{2} \rfloor < 2^\alpha + 1$ one can check that $g(t) \leqslant g(2)$ for $t \geqslant 2$.

Thus suppose that the element h, above, is a product of at t distinct transpositions with $t \geqslant 2$. Then $m \leqslant \frac{3\cdot 2^\alpha+4}{2}$. But now

$$m(m-1) = \left(\frac{3\cdot 2^\alpha+4}{2}\right)\left(\frac{3\cdot 2^\alpha+2}{2}\right) < 2^{2\alpha+3}-2 = 2(n-1)$$

and we have a contradiction. The only other possibility is that the element h is a transposition. Then we obtain that $m = 3\cdot 2^\alpha$ and so, since $\lambda > 1$,

$$m(m-1) = 3\cdot 2^\alpha(3\cdot 2^\alpha - 1) > 2^{2\alpha+3}-2 = 2(n-1)$$

which is a contradiction. Thus in both cases we obtain a contradiction and we are done. □

7. Properties of Conway groupoids

In this section we prove Theorem E and throughout we operate under the suppositions of Theorem E. Note that parts of this theorem are already known: when $\lambda = 1$ or 2, Theorem E is an immediate consequence of [12, Theorem C]. Furthermore, part (1) of Theorem E is Lemma 6.1 of [12]. Thus, to prove Theorem E we can (and will) assume throughout that $n > 4\lambda+1$ and so $G := \pi_\infty(\mathcal{D})$ is transitive.

7.1. **The imprimitive case.** In this section we suppose that G is imprimitive and that Δ is a block of size k; we will prove part (2) of Theorem E. We need the following result from [12].

Lemma 7.1. *Let $n > 4\lambda+1$ and suppose that G preserves a system of imprimitivity with ℓ blocks each of size k (so that $n-1 = k\ell$). Then at least one of the following holds:*

(i) *if $a, c \in \Omega$ lie in the same block of imprimitivity, then $\infty \in \overline{a,c}$;*
(ii) $n \leqslant \frac{6\ell}{\ell-1}\lambda + 1$.

Proof of Theorem E (2). Suppose that $n > 9\lambda+1$. We assume (for a contradiction) that G preserves a system of imprimitivity with ℓ blocks each of size k. Suppose first that case (i) of Lemma 7.1 holds and let $\Delta := \{c_1, \dots, c_k\}$ be a block of imprimitivity. Thus there exist points $d_2, \dots, d_k \in \Omega$ so that $\{\infty, c_1, c_i, d_i\}$ is a line for each $2 \leqslant i \leqslant k$. Define:

$$\Gamma := \overline{\infty, c_1} \cup \overline{c_1, d_2} \cup \overline{d_2, \infty},$$

and observe that since $\Delta \subseteq \overline{\infty, c_1}$, $\Delta \subset \Gamma$. Also note that

$$|\Gamma| \leqslant 3(2\lambda+2) - 12 + 4 = 6\lambda - 2 < n.$$

Hence we may choose $e \in \Omega\backslash\Gamma$ and define $g := [\infty, c_1, e, \infty]$. Now, $\infty \notin \overline{c_1, e}$ so that $c_1^g = e$ and since $e \notin \Delta$, we must have $\Delta^g \cap \Delta = \emptyset$. Furthermore, since $d_2 \notin \overline{c_1, e} \cup \overline{e, \infty}$, necessarily, $\Delta^g = \{e, d_2, \dots, d_k\}$. In particular (by Lemma 7.1(i)) $\infty \in \overline{e, d_2}$. But $e \notin \overline{d_2, \infty}$, a contradiction.

We conclude therefore that case (ii) of Lemma 7.1 holds, which is possible only if $\ell = 2$. This implies that G contains an element of support of size $2k = n-1$ in any generating set, contradicting the fact that G is generated by elements with support of size at most $6\lambda+2$ ([12, Lemma 7.3]). This completes the proof. □

7.2. **The primitive case.** In this section we suppose n is large enough so that, by Theorem E (2), G is primitive and we prove the remaining parts of Theorem E. We recall that, for a primitive permutation group H we write $\mu(H)$ for the minimal size of the support of a non-trivial element of G. Our strategy will be to exploit the fact that hole stabilizers naturally contain elements of small support.

We will make use of the following result of Babai [1], which is a weaker version of Theorem 6.2 that has the advantage of not depending on the Classification of Finite Simple Groups.

Theorem 7.2. *Let d be a positive integer and let H be a primitive subgroup of* $\mathrm{Sym}(d)$ *that does not contain* $\mathrm{Alt}(d)$*. Then we have that $\mu(H) \geqslant \frac{1}{2}(\sqrt{d}-1)$.*

We now prove Theorem E.

Proof of Theorem E. We have already proved parts (1) and (2): thus we must prove parts (3) and (4).

Suppose that $n > 144\lambda^2 + 120\lambda + 26$. Then Theorem E (2) implies that G is primitive. Suppose that G does not contain $\mathrm{Alt}(n-1)$. Then Theorem 7.2 and Lemma 6.8 imply that

$$6\lambda + 2 \geqslant \frac{1}{2}(\sqrt{n-1}-1).$$

Rearranging the inequality, one obtains a contradiction as required.

We are left with part (4). If $\lambda \leqslant 2$, then the result is a consequence of [12, Theorem C]. Suppose, then, that $\lambda \geqslant 3$ and that $n > 9\lambda^2 - 12\lambda + 5$. Then, in particular, $n > 9\lambda + 1$ and G is primitive. Suppose that G does not contain $\mathrm{Alt}(n-1)$.

Suppose, first, that G contains a non-trivial element of the form $g = [\infty, a, b, \infty]$ where $\infty \in \overline{a,b}$. Since the element g does not move any points on the line containing ∞, a and b, we conclude that g has support of size at most $6\lambda - 6$. Combining this fact with the inequality $\mu(H) \geqslant 2(\sqrt{d}-1)$ given by Theorem 6.2, we obtain a contradiction and the result is proved. Suppose, on the other hand, that G does contain a non-trivial element of the form $g = [\infty, a, b, \infty]$ where $\infty \in \overline{a,b}$. Then Theorem D gives the result, as for a Boolean design G is trivial. □

7.3. **The case $\lambda = 3$.** In previous work with A. Nixon [12] Conway groupoids associated with $2-(n,4,\lambda)$ designs were completely classified for $\lambda \leqslant 2$. In this subsection we discuss the possibility of extending this classification to deal with the case $\lambda = 3$.

We assume throughout this section that G is the hole stabilizer $\pi_\infty(\mathcal{D})$ of a $2-(n,4,3)$ design. We state two lemmas dealing with the different possibilities for G.

Lemma 7.3. *Suppose that G is primitive. Then either $G \cong \mathrm{Alt}(n-1)$ or one of the following holds:*

(a) $n-1 = 11$ *and* $G \in \{M_{11}, \mathrm{PSL}_2(11), \mathrm{C}_{11} \rtimes \mathrm{C}_5, \mathrm{C}_{11}\}$*;*
(b) $n-1 = 12$ *and* $G \in \{M_{12}, M_{11}, \mathrm{PSL}_2(11)\}$*;*
(c) $n-1 = 15$ *and* $G \in \{\mathrm{SL}_4(2), \mathrm{Sym}(6), \mathrm{Alt}(7), \mathrm{Alt}(6)\}$*;*
(d) $n-1 = 16$ *and G is isomorphic to one of 19 primitive subgroups of* $2^4.\mathrm{SL}_4(2)$*;*
(e) $n-1 = 27$ *and* $G = \mathrm{PSp}_4(3) \rtimes C_2$*;*
(f) $n-1 = 28$ *and* $G \in \{\mathrm{Sp}_6(2), \mathrm{Sym}(8)\}$.

Proof. Suppose, first, that G does not contain a non-trivial element of the form $g = [\infty, a, b, \infty]$ where $\infty \in \overline{a, b}$. Then Theorem 6.1 implies that $G \cong \mathrm{Alt}(n-1)$ as required.

Suppose, on the other hand, that G contains a non-trivial element of the form $g = [\infty, a, b, \infty]$ where $\infty \in \overline{a, b}$. Then G contains an element with support of size at most 12; all primitive groups containing an element with support of size at most 15 have been known explicitly since long before CFSG (see, especially, [17, 18]; we refer to the library in GAP[11] for verification).

Now, of the list provided by GAP we are able to exclude all of these groups that are not subgroups of $\mathrm{Alt}(n-1)$ and, for $n > 9$, the resulting groups are those listed in the lemma. The remaining values – when $n = 8$ or 9 – can be excluded directly since there is only one supersimple design in each case, and neither yield a primitive hole stabilizer. □

Note that Lemma 7.3 lists possible isomorphism types for $\pi_\infty(\mathcal{D})$. We do not know whether designs exist yielding hole-stabilizers of these forms.

Lemma 7.4. *Suppose that G is intransitive. Then $n = 8$ and G is trivial, or else $n = 12$ or 13. Suppose that G is transitive and imprimitive. Then $n = 9$ and $G \cong \mathrm{Alt}(4) \wr C_2$, or else $n = 13, 16, 17, 21, 25$ or 28.*

Proof. Note first that, using the Handbook of Combinatorial Designs [6]), it is easy to confirm that the two case, $n = 8$ and $n = 9$, each yield exactly one supersimple $2-(n, 4, 3)$ design. When $n = 8$ this design is the Boolean one and the associated hole stabilizer is trivial; when $n = 9$ the associated hole stabilizer is $\mathrm{Alt}(4) \wr C_2$, a transitive, imprimitive group, as required. Assume now that $n > 9$.

If G is intransitive, then the result follows from Theorem E (1). Now suppose that G is transitive and imprimitive. Then Theorem E (2) implies that $n \leqslant 28$. To complete the proof we use the fact that if a $2-(n, 4, 3)$ design exists, then $n \equiv 0, 1 \pmod 4$ and, furthermore, that, since G is imprimitive, $n - 1$ is not a prime. □

Lemmas 7.3 and 7.4 imply that the job of classifying Conway groupoids associated with $2-(n, 4, 3)$ designs is reduced to the situation where $12 \leqslant n \leqslant 29$. The number of such designs is too large to make a computer calculation feasible; a full classification will require a more detailed study of the actions listed in Lemmas 7.3 and 7.4.

References

[1] L. Babai On the order of uniprimitive permutation groups. *Ann. of Math. (2)* 113 (2): 553–568, 1981.

[2] J. Borges, J. Rifà, and V. A. Zinoviev. On non-antipodal binary completely regular codes. *Discrete Math.*, 308(16):3508–3525, 2008.

[3] ———— New families of completely regular codes and their corresponding distance regular coset graphs. *Des. Codes Cryptogr.*, 70:139–148, (2014)

[4] ———— On q-ary linear completely regular codes with $\rho = 2$ and antipodal dual. *Adv. Math. Commun.*, 4(4):567–578, 2010.

[5] A. E. Brouwer, A. M. Cohen, and A. Neumaier. *Distance-regular graphs*, volume 18 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1989.

[6] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs, Second Edition (Discrete Mathematics and Its Applications)*. Chapman & Hall/CRC, 2006.

[7] J. H. Conway. M_{13}. In *Surveys in combinatorics, 1997 (London)*, volume 241 of *London Math. Soc. Lecture Note Ser.*, pages 1–11. Cambridge Univ. Press, Cambridge, 1997.

[8] J. H. Conway, N. D. Elkies, and J. L. Martin. The Mathieu group M_{12} and its pseudogroup extension M_{13}. *Experiment. Math. 15*, 2:223–236, 2006.
[9] P. Delsarte. An algebraic approach to the association schemes of coding theory. *Philips Res. Rep. Suppl.*, (10):vi+97, 1973.
[10] J. D. Dixon and B. Mortimer. *Permutation groups*, volume 163 of *Graduate Texts in Mathematics*. Springer-Verlag, 1996.
[11] The GAP Group, `http://www.gap-system.org`. *GAP – Groups, Algorithms, and Programming, Version 4.7.4*, 2014.
[12] N. Gill, N. I. Gillespie, A. Nixon, and J. Semeraro. Generating groups using hypergraphs. To appear in *Q. J. Math.*
[13] N. Gill, N. I. Gillespie, C. E. Praeger, and J. Semeraro. Conway groupoids, regular two-graphs and supersimple designs. Preparation available at `http://arxiv.org/abs/1510.06680`
[14] M. Giudici and C. E. Praeger Completely transitive codes in Hamming Graphs. European Journal of Combinatorics **20**(7), 647 – 662 (1999)
[15] M. W. Liebeck and J. Saxl. Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces. *Proc. London Math. Soc. (3)*, 63(2):266–314, 1991.
[16] A. Mann, C. E. Praeger and Á. Seress. Extremely primitive groups. *Groups Geom. Dyn.* 1(4): 623660, 2007.
[17] W. A. Manning. The primitive groups of class $2p$ which contain a substitution of order p and degree $2p$. *Trans. Amer. Math. Soc. 4*, 3:351–357, 1903.
[18] ———— On the primitive groups of classes six and eight. *Amer. J. Math.*, 3:235–256, 1910.
[19] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.
[20] A. Neumaier. Completely regular codes. *Discrete Math.*, 106/107:353–360, 1992. A collection of contributions in honour of Jack van Lint.
[21] J. Rifà and V. A. Zinoviev. On a class of binary linear completely transitive codes with arbitrary covering radius. *Discrete Math.*, 309(16):5011–5016, 2009.
[22] ———— New completely regular q-ary codes based on Kronecker products. *IEEE Trans. Inform. Theory*, 56(1):266–272, 2010.
[23] ———— On lifting perfect codes. *IEEE Trans. Inform. Theory*, 57(9):5918–5925, 2011.
[24] D. E. Taylor. *The geometry of the classical groups*. Helderman, Berlin, 1992.
[25] M. Wertheimer. Oval designs in quadrics. In *Finite geometries and combinatorial designs (Lincoln, NE, 1987)*, pages 287–297, Contemp. Math., 111, Amer. Math. Soc., Providence, RI, 1990.

Department of Mathematics, University of South Wales, Treforest, CF37 1DL
E-mail address: `nickgill@cantab.net`

Heilbronn Institute for Mathematical Research, Department of Mathematics, University of Bristol, U.K.
E-mail address: `neil.gillespie@bristol.ac.uk`

Heilbronn Institute for Mathematical Research, Department of Mathematics, University of Bristol, U.K.
E-mail address: `js13525@bristol.ac.uk`